INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Housing Benefit & Council Tax Reduction
TO:	Head of Digital & Customer Services	**DATE:**	16 January 2024
C.C.	Chief Executive Deputy Chief Executive Head of Finance Benefits & Customer Services Manager Portfolio Holder (Cllr Harrison)		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2023/24, an examination of the above subject area has recently been completed by Emma Walker, Internal Auditor, and this report presents the findings and conclusions for information and, where appropriate, action.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and cooperation received during the audit.

2 Background

2.1 Local authorities continue to administer Universal Credit (UC) to people of working age looking for employment or on a low income. In accordance with the Localism Act 2011, the Council has adopted its own scheme for determining eligibility for Council Tax Reduction (CTR) which is incorporated into the council tax billing process.

2.2 There exists a Memorandum of Understanding (MoU) between the Department for Work and Pensions (DWP) and Warwick District Council (WDC). The MoU sets out the framework and operating policy through which WDC can access and use DWP, HM Revenue and Customs (HMRC) and Home Office data.

2.3 At the time of the audit, the applications and supporting evidence for Council tenant, Housing Rent Account and non-Housing Rent Account claims were being externally audited. Following discussion between the assignment auditor, the Audit & Risk Manager, and the Principal Internal Auditor, it was felt that, to avoid duplication of work, the assignment would benefit from a different scope, one that focused on the MoU. Subsequently, it was agreed with the auditee, the Benefits & Customer Services Manager, that the audit would comprise a review of the MoU to ascertain whether there are adequate controls in place to ensure that claimant data received from the DWP, HMRC and/or the Home Office is appropriately accessed, handled, exchanged, and protected.

2.4 It should be noted that the DWP are aware that not all Local Authorities will be compliant with the requirements laid out in the MoU. Where WDC is non-compliant, the DWP have offered to work with the Council to rectify these issues.

3 Objectives of the Audit and Coverage of Risks

3.1 The management and financial controls in place have been assessed to provide assurance that the risks are being managed effectively. It should be noted that the risks stated in the report do not represent audit findings in themselves, but rather express the potential for a particular risk to occur. The findings detailed in each section following the stated risk confirm whether the risk is being controlled appropriately or whether there have been issues identified that need to be addressed.

3.2 In terms of scope, the audit covered the following risks:

1. Risk of incurring financial penalties for not adhering to the Memorandum of Understanding.
2. Risk of non-compliance with key legislation or legal requirements.
3. Risk of sensitive data being breached/leaked.
4. Risk of IT systems being non-compliant with government regulation.
5. Data not passed onto DWP within specified timescales.
6. Provision of incorrect information/advice to benefit claimants.
7. Inadequate training on systems/the benefit assessment process.
8. Officer roles and responsibilities not clearly defined.
9. Council properties not advertised in a timely manner/property information inaccurately published.
10. Lack of data retention policy in place.
11. Staff inappropriately vetted with access to customer data.
12. Officers accessing data whilst agile working.
13. Loss of IT system.
14. Loss of key records.

3.3 A 'risk-based audit' approach has been adopted, whereby key risks have been identified during discussions between the Internal Auditor and key departmental staff. The Significant Business Risk Register has also been reviewed.

3.4 These risks, if realised, would be detrimental to the Council with regards to meeting the internal 'Services' element of the Fit for the Future Strategy. The Council has a duty to focus on customer needs and increase the provision of digital services.

4 Findings

4.1 Recommendations from Previous Reports

4.1.1 The current position in respect of the recommendations from the previous audits undertaken in November 2018, and September 2021 were also reviewed. The current position is as follows:

Recommendation	Management Response	Current Status
Staff should be reminded of the need for Senior Officers to review the cases and complete the relevant decision notices. (November 2018)	To be discussed during the next team meeting.	Completed.
Staff should be reminded of the need to get the claimants approval for the benefit payments to be made to their landlords in all relevant cases. (November 2018)	To be discussed during the next team meeting.	Completed.
Staff should be reminded of the need to select the relevant reason codes when processing landlord payment applications. (November 2018)	To be discussed during team meeting.	Completed.
Sample testing of changes to universal credit should be undertaken to ascertain if the DHPs need to be amended. (September 2021)	The Benefits and Customer Services Manager will request that the Benefits Team Leaders undertake a percentage check for accuracy. The results should be reviewed after three months to determine whether more in-depth checking is required.	A percentage accuracy check has been undertaken and there were some cases where a customer had a change in circumstances and had not notified WDC. Notifications sent to customers have been amended to place more emphasis on their duties to inform WDC of any changes in circumstances. These checks are undertaken by the Benefits Team Leaders.

4.2 **Financial Risks**

4.2.1 **Potential Risk: Risk of incurring financial penalties for not adhering to the Memorandum of Understanding.**

The Benefits & Customer Services Manager (BCSM) advised that there are currently no management reviews performed on claims to ensure that work is conducted in line with the MoU.

Recommendation – Management reviews should be regularly performed on the benefit assessment process to ensure compliance with the MoU.

The MoU is reviewed every year and once updated, is signed by the S151 Officer and BCSM. The Chief Executive is not expected to sign the document but is expected to declare that he has understood the obligations contained within it.

The latest revision of the MoU contains several changes, including:

- Rights related to automated decision-making including profiling.
- LA staff training.
- PSN update.
- Configuration and change management.
- Anti-Malware.
- Use of live data in testing.
- EAS tokens.
- New data sharing data re-use assessment template.
- Additional searchlight access.
- Updated definition of local welfare provision and household support fund addition.
- VEP2a extract from LAs to the Housing Benefit Information Service.
- New changes to accessing the income tab on searchlight.
- Security standard – use of cryptography.
- DWP data-share summary table.
- Cryptographic compliance LA signatory.

There is a signature missing from the BCSM on the MoU relating to Annex F – Single Housing Benefit Extract.

Recommendation – All signatures should be provided on the MoU.

The Apollo Register currently provides the DWP staff with a list of staff in the Authority who are authorised to obtain DWP data, without requiring customer permission. The Benefits Teams Leaders (BTL) maintain this register as the DWP often ask for updated versions. It should be noted that the Appollo Register is used for the purpose of legacy benefits and not for UC. It is an offence to access or process DWP data for any purpose other than that which is outlined in the DWP Apollo Register Guidance. Staff members are reminded that they must only utilise the Apollo Register for the services that they are entitled to access for customer data, when unable to do so on Searchlight. Information obtained via the Apollo Register is treated as 'official' and must adhere to GDPR and Data Protection Regulations. Benefits staff have to undergo relevant Pre-Employment and Government Baseline Personnel Security Standard (BPSS) checks prior to utilising the Apollo Register. The register was last reviewed and signed by the BTL in May 2022. Local authorities are reminded to conduct quarterly reviews of the members of staff who have access to the Apollo Register, informing the DWP of any changes which require updating.

Advisory – Consideration should be given to reviewing the Appollo Register on a quarterly basis.

Recommendation – Staff should be asked to declare, annually, that they have read and understood the terms and conditions laid out in the register.

A list of changes to the MoU was examined by the auditor to ensure that these had been reflected accurately in WDC Policy. The review noted that six of the seven changes had been reflected in WDC policies and procedures. All pieces of legislation quoted in the MoU had also been suitably referred to in several Council policies, including the Data Handling Policy, Data Protection and Privacy Policy, Data Protection when Agile-Working Policy and Data Retention Policy. Legislation applicable to the MoU is also referred to in the administration of the CTR scheme and Housing Benefit Privacy Notice.

4.3 Legal and Regulatory Risks

4.3.1 Potential Risk: Risk of non-compliance with key legislation or legal requirements. (SBRR)

The MoU refers to several key pieces of legislation that must be adhered to including the Data Protection Act 2018, the Homelessness Reduction Act 2017, the Social Security Administration Act 1992, and the Welfare Reform Act 2012. Guidance is issued by the DWP, and the Council then sets its own policies based on this guidance. Updates to guidance and circulars are sent to the BCSM before being circulated to the team; circulars are publicly accessible through Gov.uk and outline the steps to be taken in various scenarios. Changes to Universal Credit allowances 2023/24 have been compiled by the Principal Benefits Officer (PBO) and made available in the network files; these are updated annually.

Whilst a formal training manual does not exist, The Benefits Directory is used as the main basis for training. This is a subscription service that all benefit assessment staff have access to. It is a repository for all the information that an assessment officer requires in order to assess UC and CTR. The Benefits Directory website reflects any changes in legislation and provides introductory and ongoing training relating to regulations and DWP circulars. Notes from the directory focus on topics such as Exempt Accommodation, Care Homes, DWP Guidance and Supported Housing.

Training itself is a graduated process that is documented as it progresses; this is stored in a secure folder that only the BCSM, PBO and BTL can access. There is also training on the use of CIVICA; this typically takes the trainee through an introduction to its general use before gradually building up their knowledge with more complex tasks until they are able to assess new claims and changes in circumstances.

4.3.2 Potential Risk: Risk of sensitive data being breached/leaked.

There is limited separation of duties in terms of benefit assessments; Benefit Assessment Officers (BAO) will invariably input and assess the same claims, especially those on electronic forms. However, there is a segregation of duties in place between the Systems Officers, who process the payments, and the BAOs.

The CIVICA app, through which claims are assessed and monitored, is restricted to authorised users only. Benefit assessment staff have direct access to the DWP Searchlight system that contains DWP and HMRC data. Other information is received through the TYF (Transfer Your Files) portal and uploaded onto CIVICA. Pension information can be obtained directly in real time, and earnings and

private pension information can be obtained through VEP (Verify Earnings and Pensions) or RTI (Real Time Information); details of a person's immigration status can be obtained from the Home Office. The data that is held within the Benefit modules on CIVICA is largely derived from the DWP and HMRC, which is provided for the effective administration of UC and CTR.

Each year, WDC sign the MoU to confirm that they comply with the law in relation to how the data is accessed, stored, and used. The consequences of misusing the data could potentially lead to disciplinary action against the individual and therefore it is important that everyone with access to the CIVICA Benefits module is aware of their responsibilities. All Benefits staff must now be vetted against the BPSS. As of April 2011, if an existing employee is newly assigned to a post where access to government assets is necessary, they will be subject to BPSS verification checks. All new recruits who have access to DWP, HMRC and/or Home Office data are also subject to BPSS checks. The DWP does not, however, require BPSS checks to be applied retrospectively for existing staff where pre-employment checks have already been carried out prior to April 2011.

As per the WDC Data Handling Policy, users should not be allowed to access information until System Owners are satisfied that they understand and agree the legislated responsibilities for the information that they will be handling. System access is, therefore, granted to authorised users only. There is now a form on the Intranet that staff who wish to access data held on the CIVICA Benefits system must complete. In July 2023, the Systems Officer requested that all existing CIVICA users complete the new access request form.

Housing Benefit is administered under the Social Security Administration Act on behalf of the DWP and therefore much of the data held in the system belongs to them. The Council is allowed to provide access to this data only for certain purposes where it is specified that they have permission in legislation to do so. To enable this, the Council is provided with a set number of concurrent licences. This means that if concurrent use of the system is at the maximum, then no further access to the system is granted until a user "logs-out." Users are, therefore, updated as and when they leave WDC or change job roles and no longer require CIVICA access. Users requesting access are also mandated to comply with a confidentiality agreement. The Systems Officer will be completing a review of all users in six months' time. In addition to this, in July 2024, all users will be asked to complete a new CIVICA access form, as a reminder of the confidentiality agreement, and to check that their Declaration of Interests has not changed.

The CIVICA system provides a full audit trail of who has accessed information; Searchlight access is also subject to random testing checks. The BTL conducts audit checks of Searchlight to ensure that DWP data is accessed only for lawful purposes. The BCSM has to send a list of daily test checks to the BTL who then verifies that DWP data has been accessed for a valid reason; details of these tests are then sent to the DWP. A CIVICA user review was conducted in August 2023; any users with no relevant business need, who had either changed role or left the organisation, had their login disabled in order to protect information.

Staff have received data protection training, as well as training on how to report and respond to data breaches; however, no training on this has taken place since 2021.

Recommendation – In line with the MoU, yearly refresher training should be conducted on data protection and responding to data breaches.

The BCSM advised that there have been no data breaches related to the DWP. Although there have, in the past, been data breaches related to Council administration e.g., letters addressed to separate claimants being sent in the same envelope, this has not occurred for some time.

Claimants are made aware of how their data will be used and stored through the Privacy Notices on the Internet. Personal data is used to assess entitlement to Housing Benefit and/or CTR and/or Discretionary Housing Payments. The legal basis for this processing is contained within the Social Security Administration Act 1992, the Social Security Contributions and Benefits Act 1992, the Local Government Finance Act 1992, and the Discretionary Financial Assistance Regulations 2001. In order to assess entitlement to Housing Benefit, the Council needs to undertake a means test and therefore will collect information about income, savings, capital, and circumstances of other people who reside in the same property as the claimant. Although claimants have the right not to provide this information, if they elect not to do so, benefit will not be awarded. WDC also collect and share information with the DWP, HMRC, other local authorities, other Council departments and in some cases, landlords where the law allows it. WDC share information with other Council departments, for example Electoral Services to allow them to complete their statutory duties (as laid out in Regulations 23, 35 and 35A of the Representation of the People (England and Wales) Regulations 2001). Claimants are entitled to request a copy of any information about them that the Council holds. If the information is inaccurate, claimants have the right to have this corrected.

The Systems Officers receive the Council Leavers list so that they can disable access for staff leaving the organisation. Only BAOs have access to the systems outlined in the MoU, although the BCSM will share safeguarding information where appropriate as this is negated by the Data Protection Act 2018.

Advisory – Consideration should be given to stipulating in the Council leavers letter that any member of the Benefits team has a duty to uphold confidential obligations regarding the data they have accessed/information they have processed.

All BAOs have been allocated a unique EAS token number to access DWP data; old EAS token numbers are deactivated to prevent unauthorised access to information. The EAS spreadsheet displays who has access to Searchlight as well as the Tell Us Once function and VEP. Some officers have access to the TYF module, a system which allows officers to download information from the DWP system or upload necessary information to the database. EAS tokens have to be approved either by the BCSM or the PBO. EAS tokens belonging to the BCSM and PBO have to be approved by the DWP.

Recommendation – The EAS spreadsheet needs updating as this refers to officers who either no longer work for the organisation or officers who have transferred to other service areas.

4.3.3 **Potential Risk: Risk of IT systems being non-compliant with government regulation.**

There have been no changes to the way that DWP data is transmitted; the network has remained the same apart from routine upgrades. DWP data is stored on an on-prem environment which is essentially infrastructure running within the confines of the organisation, meaning that WDC has absolute control over its data and data remains in a private network. A Public Services Network (PSN) check took place on 10 March 2023 and is not due to expire until 10 March 2024. This is a health check in which any major flaws have to be rectified and certified before the PSN submission can be sent to Gov.uk. There is a filtering system in place which inspects incoming emails; any that are suspect or have questionable attachments are either quarantined or deleted depending on the severity. If an email is quarantined, the user is sent an alert and has to request a release from ICT.

WDC are not currently meeting some of the standards for encrypted information at rest, as outlined in the MoU. This is essentially the practice of protecting data that is stored on a backup device. Where applicable, the master encryption key must reside within assured cryptographic hardware. Information encrypted at rest must also be integrity protected. The encryption software deployed on devices must require sufficient entropy as part of the authentication mechanism. In a scheme that uses a password as the authentication mechanism, this equates to a password that is of sufficient length and complexity. All data on portable computer devices must be, where possible, encrypted. If this is not possible, then all confidential, restricted, or personal data held on the portable device must be encrypted.

Encryption software deployed on devices (i.e., laptops, portable storage devices) must restrict the number of authentication attempts within any given time interval. CIVICA will lock the user out of the system after three failed attempts to log in. All Council-owned mobile devices that store Council data have disk encryption. Council-owned Windows laptops and tablets are also encrypted with BitLocker. ICT Services deploy an up-to-date anti-malware signature file to all users who work away from WDC premises. Users who work remotely must ensure that their portable computer devices are connected to the corporate network to enable the anti-malware software to be updated.

The Council is also non-compliant in using live data in test systems for testing purposes. Whilst the data used for testing is controlled to the same standards as the live CIVICA system, this is seen as a temporary solution and ideally needs to be brought in line with DWP standards. Local Authorities must not use live DWP, HMRC and/or Home Office derived data for the purpose of testing their system updates and/or improvements. As best practice, DWP requires Councils to use a test system which contains synthetic data that can be updated and tested prior to releases. If Councils are unable to develop a synthetic data solution to be used in a testing environment, then they are permitted to use anonymised, cloned, or mirrored DWP, HMRC and/or Home Office data.

Recommendation – A test system, containing anonymous or synthetic data, should be used to test and update information before being released in the live system.

Recommendation – An assessment should be carried out, ensuring that use of cryptography meets Government Security Standards, in line with the requirements of the MoU.

The Council is currently meeting the standards for encrypted data in transit, as data is downloaded and immediately uploaded to CIVICA before being deleted. The DWP do not switch off data for non-compliance, unless in extremis, for example, if there was an ongoing cyber incident. Unless there is a catastrophic risk associated with WDC, the DWP will not terminate their data sharing.

4.3.4 **Potential Risk: Data not passed onto DWP within specified timescales.**

Housing Benefit debt recovery data is run through CIVICA by the Systems Officer and uploaded to the DWP by the BTL on a monthly basis. Data gleaned from the Single Housing Benefit Extract (SHBE) is uploaded monthly by the Systems Officer. The Council must submit their monthly data on their scheduled transfer date as per the agreed SHBE timetable. If an extraction is not received on the scheduled transfer date, a standard email reminder is issued to the Council. SHBE returns received after the agreed monthly cut-off point cannot be accepted and where this occurs, WDC will be advised, and the data will be deleted. SHBE data sent to the DWP is retained for a few weeks in case there is an issue with the data; at the time of the audit, the last extract was sent on 11 October 2023 and aligns to the SHBE 2023/24 specification issued by the DWP.

4.4 **Reputational Risks**

4.4.1 **Potential Risk: Provision of incorrect information/advice to benefit claimants.**

All eligibility criteria and details on how to claim benefit are outlined on the Council's website. Staff are made aware of changes to eligibility criteria through DWP circulars or team emails. Applicants can apply for CTR alongside UC. UC is one monthly payment for the household, paid directly into a bank account. This includes rent but disability allowance or CTR must be claimed separately as UC does not contribute towards council tax. Applications are assessed and calculated with reference to their circumstances, income, and capital. Applicants can check their eligibility through the benefits calculator linked to the WDC website.

CTR is a scheme local to Warwick District; those not eligible for CTR may be eligible for discounts or exemptions. CTR is awarded if the applicant is on low income, has to pay council tax or if their savings are less than £16,000 for the banded scheme. Second adult rebate is for those of pension age who cannot get help for themselves with their council tax but have people living with them that are on low incomes; this is not available for those of working age.

Most applications are completed online through forms on the WDC website or over the phone with the Customer Service Team. E-forms are available on the

Council's website to submit applications, report changes in circumstances and check claim status. The Benefits team maintain a spreadsheet outlining the number of electronic forms and paper forms received. As of September 2023, 164 forms were received, 82% of which were electronic. Claimants are presented with a list of requirements needed to apply for UC, although the application itself is completed through the Gov.uk website. Claimants are able to save their application and return at a later date if desired. The WDC website provides a video, transcript, and useful contacts in order to provide help and advice to claimants.

The CTR form is easily accessible and completed through the Council's website. Claimants are reminded of the evidence needed to hand before starting a new form. The WDC website contains a benefits page that can be accessed from the home page. This displays the contact e-mail address and telephone number of the Benefits team. Opening times of Riverside House are published on the website, although not linked to the benefits pages.

Advisory – Consideration should be given to including a link to the 'Contact Us' page on the website benefits pages.

Advice lines such as the UC helpline and Citizens Advice are advertised through the website. Home visits can be conducted by the Revenues Visiting Team if claimants need to complete a paper form, or evidence is needed to be collected; however, these are rare and most applicants struggling to complete the form go through the process with a BAO over the phone. Customer service officers receive training on the various benefits for which applicants can claim, but they are not permitted access to Searchlight.

The BTL advised that if an 'appeal' is raised against a refused application, the other BTL would review the application to ensure that the decision reached is appropriate. In terms of the refused applications, reports can be obtained from CIVICA to see which claims have been refused. A list of refused applications across the financial year 2023/24 was collated from the CIVICA system. These were then investigated by the auditor to ensure that a reason for refusal had been provided to the claimant. In all twenty of the applications sampled, a reason had been provided to the claimant and evidence of this had been uploaded to CIVICA accordingly. Refusals were, however, provided fairly inconsistently in terms of timescales, but this is largely dependent on how quickly BAOs can assess claims.

4.4.2 **Potential Risk: Inadequate training on systems/the benefit assessment process.**

Staff receive CIVICA system training and training on the DWP Searchlight system. Staff have to pass the Searchlight training and receive a certificate before they can gain access to the data held on the system. Searchlight also asks various questions of the user before they login and will deny access to the user unless the questions have been answered correctly.

Procedure notes are compiled in order to help BAOs assess claims. Recently compiled notes included instructions on how to create an external address and how to prepare to delete old claims from the system; these notes were last

modified in October 2023. Guidance has also been collated regarding loading Housing Benefit Matching Service (HBMS) data onto CIVICA in line with the circular issued by the DWP in March 2023.

Training notes are in place for CTR assessment using UC which were last updated on 24 April 2023 to incorporate the updated banded scheme. The scheme is designed to give a percentage discount from council tax, based on the calculated income of the taxpayer and their circumstances. There are also training notes on UC Batch processing, specific CIVICA module instructions, and UC Balancing Reports. Currently staff do not receive yearly refresher training regarding the Searchlight system.

Recommendation – Yearly refresher training on Searchlight data should be given to benefits staff, as outlined in the MoU.

Staff 1:1s take place in the form of conference calls with the relevant BTL on a bi-monthly basis; each BTL has five BAOs reporting to them. Team meetings take place amongst the respective teams on a weekly basis. Whole team meetings are then conducted monthly to discuss any changes to the assessment process or to specific legislation. Minutes are distributed via email and include topics such as system checks, rent officer referrals, work performance, and WDC-related updates such as the move to the new offices. Any relevant training notes are also distributed in this manner.

4.4.3 **Potential Risk: Officer roles and responsibilities not clearly defined.**

It is the responsibility of the Chief Executive Officer and S151 Officer to ensure that the requirements within the MoU are communicated to all staff who have access to DWP, HMRC and/or Home Office data. The Council must seek assurance from their staff members, highlighting that they understand their personal roles and responsibilities when handling DWP, HMRC and/or Home Office data. At present, the BAOs do not receive a copy of the MoU.

Recommendation – All members of the Benefits team should read the MoU and sign a declaration form to acknowledge that they understand their role and responsibilities. This should be done on a yearly basis, in line with the MoU updates.

Recommendation – Reminders relating to the confidentiality of information obtained through the DWP should be regularly issued to the Benefits team.

4.5 **Fraud Risks**

4.5.1 **Potential Risk: Lack of data retention policy in place.**

The Council must ensure that it has written data retention schedules, policies, processes, and procedures in place to identify when data made available by the DWP is due for deletion and/or destruction and remove such data when it is no longer required. The Council must also ensure that it is able to provide written assurances to the DWP that data has been deleted and/or destroyed within the

defined data retention schedule and policy periods; however, the BCSM advised that the DWP have never asked for evidence that data has been destroyed.

Advisory – Consideration should be given to providing assurance to the DWP that data has been destroyed in line with data retention schedules.

According to the data retention policy, WDC will keep data for six years after a claim has been closed; however, there may be circumstances where data needs to be kept for longer, for example if the claimant has been overpaid and owes the Council money.

4.5.2 **Potential Risk: Staff inappropriately vetted with access to customer data.**

Officers in the Benefits team are expected to declare any financial interests and, separately, whether they are a landlord or owner of a property within the district. They are also prevented from dealing with their own council tax accounts or benefit claims through CIVICA.

A list of officers from the Benefits team was collated from the Intranet. These were then used by the auditor to check that any potential conflict of interests with claimants had been suitably declared. In nine cases, the officers' surnames produced a match with live claims on the system. These were then reference-checked against claimant addresses where there were found to be no correlations. It was also confirmed by the auditor that no claims had been processed by officers with surname matches.

The Security Policy Framework describes the Cabinet Secretary and the Official Committee on Security expectations of how HM Government (HMG) organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently, and securely. Although the Security Policy Framework was not mandated for local government, the DWP does require Local Authorities to align with the Government Security Classifications scheme and protect information accordingly. The Security Policy Framework stipulates that recruitment checks will be made in line with the BPSS for those with access to HMG assets. Staff are vetted against the BPSS and not granted access to any systems, information or databases until these checks have been passed. The BTL is able to verify these BPSS checks to ensure that they are legitimate. Council staff who transfer to roles where access to government data is necessary also undergo the same verification checks.

The Customer Services Team (CST) have access to CIVICA for reference use only but are not permitted to share Benefit information with Council Tax; members of the CST are also vetted against BPSS.

4.5.3 **Potential Risk: Officers accessing data whilst agile working.**

There is a WDC remote-working policy in place, but this has since been replaced by the Agile-Working Guidance, which makes no mention of the Security Policy Framework. Home and remote working is permitted as long as any solution complies with the Security Policy Framework and compliance standards as

referenced in the MoU. The Council Remote Working policy reminds staff that under no circumstances should non-Council owned equipment be used to access PSN facilities. The policy reminds staff to report loss or theft of equipment to ICT, not leave laptops unattended, not install or update any software/hardware onto Council laptops, report any faults and not keep RSA tokens in the same location as the laptop. No family members or friends may use Council-owned IT equipment. If privately-owned ICT equipment is used to produce Council-related documents, or is used to access systems such as e-mail, then the employee or Member is responsible for ensuring that all such documents and any downloaded data is stored securely or deleted. Any user accessing PSN type services or facilities, or using PSN protected or restricted information, must only use Council-owned equipment that has appropriate technical security and advanced authentication mechanisms whilst working remotely.

In the home, equipment should be located out of sight of the casual visitor and other family members. For home working it is recommended that the office area of the house should be kept separate from the rest of the house. Equipment must be secured whenever it is not in use. Portable computer devices should be switched off, logged off, or password protected when left unattended. Dual-factor authentication must be used when accessing the Council network and information systems remotely via Council-owned and non Council-owned equipment.

There is no specific security training for staff working from home, as this is covered under the corporate agile-working guidance. WDC is committed to ensuring compliance with its obligations under UK GDPR. All employees should abide by WDC's Data Protection Policies and Procedures. WDC retains the right to withdraw agile working arrangements if data confidentiality is not maintained. Whether working from a public location, a Council work setting or in the home environment, there is a need to keep data safe and to be aware of having confidential conversations outside of Council settings even in the home environment with other people present. If individuals work with sensitive data or information, a privacy screen should be supplied by line managers.

Advisory – Consideration should be given to assessing the home-working environments of Benefits staff and providing privacy screens where applicable.

Printing of data at home is not permitted on non WDC equipment. If working from home or at another location, the working environment must be suitable, free of interruptions and with a suitable workspace and technology to enable effective communication and have due regard to confidentiality. All individuals have an implied duty not to disclose confidential information or use it for any purpose other than WDC's business.

The MoU states that if the Council wishes to use data made available by DWP for another purpose than that for which it was originally intended, it must complete the data sharing re-use assessment template. If Councils wish to make a request to re-use data, they will need to identify both an appropriate lawful basis (under article 6 of the UK GDPR) and a statutory power in order to process personal data made available by the DWP. It is a DWP policy decision that Councils cannot re-use data for any other purpose until they have completed the

data sharing re-use assessment template and received a response from the DWP. This allows the DWP to understand the legal gateway and lawful basis the Council is relying upon and also to ascertain whether there are reputational risks involved with the re-use request. Permission will need to be sought directly from HMRC, in relation to any re-use requests for data derived from HMRC. Where HMRC data has been made available to WDC for a purpose described in the MoU, it may not be re-used for another purpose unless the law allows it. The Council is, however, permitted to re-use CTR data that they hold during Valuation Tribunals or Valuation Appeal Committees. WDC can re-use data supplied for CTR purposes for the purpose of determining whether a person applying for or receiving the provision of domiciliary care or residential care is liable to contribute towards the cost of that care and, if so, the amount of that contribution. WDC can re-use the data supplied for CTR purposes for the purpose of determining whether to make a Discretionary Housing Payment and, if so, the amount of the payment.

4.6 Other Risks

4.6.1 Potential Risk: Loss of IT system.

WDC systems are subject to regular backups and testing. Once backed-up, system data is retained for up to a year. Periodically, IT will test the ability to restore systems entirely from backups, some of which are air-gapped from the online environment. If the current systems were to be totally lost, these offline backups could be used to restore previous versions of the data.

4.6.2 Risk: Loss of key records.

Hard documents are scanned in by the CST and held for a month. This is to ensure that if the scan is of poor quality or extra information is needed, that the BAOs can still obtain this information; original documents are sent back to the claimant immediately. All files are uploaded to CIVICA as is information from the DWP, which is uploaded to CIVICA and then deleted.

According to the Government Security Classifications (GSC) policy, everyone who works in or with the government (including staff, contractors, and service providers) has a duty of confidentiality coupled with a responsibility to safeguard any HMG information or data that they access and/or share, and they must be provided with appropriate training. All HMG information should, where possible, be clearly marked with a classification tier. The majority of information that is created, processed, sent, or received in the public sector and by partner organisations, which could cause no more than moderate damage if compromised should be classed as 'official'. A 'sensitive' marking should be applied to official information that is not intended for public release. Official information or material marked 'sensitive' is likely to cause moderate damage to the work or reputation of WDC and/or HMG and must, therefore, be marked with the 'sensitive' marking.

The GSC Policy includes a list of handling instructions delineating each piece of information that should be marked. The policy also includes guidance on remote-working. When working remotely, users must protect information to the same standard as when working in the office. Hard-copy documents must only

be taken outside the office in exceptional circumstances with the appropriate approval for information of that sensitivity.

A list of current benefit applications was collated from the CIVICA system. These were then investigated by the auditor to ensure that diary notes containing DWP-related content had been marked as confidential. The nature of the diary notes related to either Home Office documentation, immigration status, resident refugee permits, power of attorney, deed of name changes, the EU settlement scheme, or direct data from the DWP. In fourteen cases, the diary notes had been marked as 'severe', but not 'confidential'. One case related to data from the DWP regarding a vulnerable claimant which had been designated a 'normal' status diary note. As only accredited users can access the system, and diary notes are marked as 'severe', this did not present a major issue. However, system notes could be brought in alignment with the GSC Policy and marked as 'confidential' or 'official'.

Advisory – Consideration should be given to marking all DWP/HMRC related documents, and any relevant correspondence as either confidential or official.

The Council's Data Handling Policy outlines that a protective marking scheme should be used to label, store, handle and dispose of data, in accordance with relevant legislation and government standards. Information created and received by the Council should be classified (protectively marked) according to the sensitivity of its contents.

The protective markings to be used by employees are:

- PUBLIC or no marking. Anyone can access the information internally or externally. It may be published on the web or in paper form (but may still be copyright and chargeable).
- INTERNAL - Anyone can access the information internally. It should not be published on a public website or generally released outside WDC.
- CONFIDENTIAL (PROTECT) - Information where disclosure or unauthorised access would be inappropriate, inconvenient or cause harm or financial impact.
- RESTRICTED - Information to be restricted at a higher level of assurance than Confidential, due to significant inconvenience, damage, harm or financial impact on the Authority or individuals. This marking applies to the holding, storage and transmission of bulk customer or employee records and access will be restricted.

When protective marking is required, it should be clearly displayed, in bold, in the centre of the header and footer on each page of the document or diary note. Protective markings must be reviewed during the life of the information or document to ensure that the marking is appropriate and relevant. Applying too low a protective marking may lead to damaging consequences if the document is not sufficiently protected and can be accessed by those who should not see it. Applying too high a protective marking could mean that those who need to have access to a document are not authorised to do so and could lead to unnecessary and expensive protective controls being put in place.

All Council information which contains personal data should be, as a minimum, classified as 'confidential' according to the Data Handling Policy. Where personal information is subject to electronic transmission, such as e-mail, the information must be encrypted. The WDC Data Handling Policy contains a table which defines how each information resource can be handled, transmitted, stored, and disposed.

5 Summary and Conclusions

5.1 Section 3.2 sets out the risks that were reviewed as part of this audit. The review highlighted weaknesses against the following risks:

- Risk 1 – The Apollo Register and benefit claims may not be reviewed by management in line with the MoU.
- Risk 3 – The EAS spreadsheet is out of date and refresher training is not provided on data protection.
- Risk 4 – Synthetic data is not being used to test systems; cryptography standards are not in line with government regulations.
- Risk 7 – Refresher training on Searchlight is not provided.
- Risk 8 – Staff may be unaware of their roles and responsibilities or confidentiality obligations.

5.2 Further 'issues' were also identified where advisory notes have been reported. In these instances, no formal recommendations are thought to be warranted, as there is no significant risk attached to the actions not being taken.

5.3 In overall terms, therefore, we are required to give a MODERATE degree of assurance that the systems and controls in place in respect of the Housing Benefit & Council Tax Reduction are appropriate and are working effectively to help mitigate and control the identified risks.

5.4 The assurance bands are shown below:

Level of Assurance	Definition
Substantial	There is a sound system of control in place and compliance with the key controls.
Moderate	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited	The system of control is generally weak and there is non-compliance with controls that do exist.

6 Management Action

6.1 The recommendations arising above are reproduced in the attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit and Risk Manager

Appendix A

Action Plan

Internal Audit of Housing Benefit & Council Tax Reduction– January 2024

Report Ref.	Risk Area	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.2.1	Financial Risk - Risk of incurring financial penalties for not adhering to the Memorandum of Understanding.	Management reviews should be regularly performed on the benefit assessment process to ensure compliance with the MoU.	Medium	Systems Officer; Benefits and Customer Services Manager	Compliance checks will be recorded when each new CIVICA release/patch is installed. Compliance checks will be recorded for any change of process.	Ongoing.
		All signatures should be provided on the MoU.	Low	Benefits and Customer Services Manager	The new MoU is shortly due to be issued. The Benefits and Customer Services Manager will ensure all signatures are provided.	30th April 2024
		Staff should be asked to declare, annually, that they have read and understood the terms and conditions laid out in the register.	Low	Benefit Team Leaders; Benefits and Customer Services Manager	A training document has been produced. This will be issued to all staff, and we will use meta compliance to confirm that staff have read and understood the conditions.	31st January 2024 and annually thereafter
4.3.2	Legal & Regulatory Risk: Risk of sensitive data being breached/leaked.	In line with the MoU, yearly refresher training should be conducted on data protection and responding to data breaches.	Low	Benefit Team Leaders; Benefits and Customer Services Manager	A training document has been produced. This will be issued to all staff, and we will use meta compliance to confirm that staff have read and understood the conditions.	31st January 2024 and annually thereafter

Report Ref.	Risk Area	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
		The EAS spreadsheet needs updating as this refers to officers who either no longer work for the organisation or officers who have transferred to other service areas.	Medium	Benefit Team Leaders	The up-to-date version had been saved on a desktop and had not, therefore, been made available for the audit. This has been addressed and staff have been advised not to save items locally.	Complete.
4.3.3	Legal & Regulatory Risk: Risk of IT systems being non-compliant with government regulation.	A test system, containing anonymous or synthetic data, should be used to test and update information before being released in the live system.	Medium	Benefits and Customer Services Manager; Exchequer Manager	Please see response from DWP regarding the issues with having a test system with synthetic data. Access to the test system is currently controlled to the same level as the live system.	TBA
		An assessment should be carried out, ensuring that use of cryptography meets Government Security Standards, in line with the requirements of the MoU.	Low	Head of Customer & Digital Services	An assessment will be completed.	31 May 2024
4.4.2	Reputational Risks: Inadequate training on systems/the benefit assessment process.	Yearly refresher training on Searchlight data should be given to Benefits staff, as outlined in MoU.	Low	Benefit Team Leaders; Benefits and Customer Services Manager	A training document has been produced. This will be issued to all staff, and we will use meta compliance to confirm that staff have read and understood the conditions.	31st January 2024 and annually thereafter

Report Ref.	Risk Area	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.4.3	Reputational Risk: Officer roles and responsibilities not clearly defined.	All members of the Benefits team should read the MoU and sign a declaration form to acknowledge that they understand their role and responsibilities. This should be done on a yearly basis, in line with the MoU updates.	Low	Benefit Team Leaders; Benefits and Customer Services Manager	The MOU contains information that is not relevant to all staff. There is a risk that in giving them the full MoU to read, emphasis on the relevant areas will be lost. Therefore, a training document has been produced. This will be issued to all staff, and we will use meta compliance to confirm that staff have read and understood the conditions.	31st Jan 24 and annually thereafter
		Reminders relating to the confidentiality of information obtained through the DWP should be regularly issued to the benefits team.	Low	Benefit Team Leaders; Benefits and Customer Services Manager	A training document has been produced. This will be issued to all staff, and we will use meta compliance to confirm that staff have read and understood the conditions. Confidentiality will also be put on the team meeting agendas.	31st Jan 24 and annually thereafter

* The ratings refer to how the recommendation affects the overall risk and are defined as follows:

High: Issue of significant importance requiring urgent attention.
Medium: Issue of moderate importance requiring prompt attention.
Low: Issue of minor importance requiring attention.