**Internal Audit Report
2013/14**

**Records Management & Data Quality in the
Contact Centre**

**Ann Kirk & Julie Ball
19 May 2014**

Contents

Audit: Records Management & Data Quality in the Contact Centre

Auditor: Ann Kirk & Julie Ball

If viewing on-screen, please click on the links below or use the scrolling arrows

1   Introduction

1.1   In order for the Council to carry out their responsibilities it is necessary that data and information be collected from members of the public and various other sources.

1.2   Records Management is the practice of maintaining the records of an organisation from the time they are created up to their eventual disposal. This may include classifying, storing, securing and destruction or in some cases archival preservation of records.

1.3   Data makes up records of information and is an asset to the organisation, but only if it is accurate and fit for purpose. There could be a potential breach of the Data Protection Act with financial consequences if the data is inaccurate and poor decisions are made.

2   Scope

2.1   The Council's Customer Services Centre is the first port of call for customers conversing with the council whether over the phone or face to face. The service deals with a number of queries from the public for a number of services across the council using their Customer Records Management System. As a consequence this audit focuses on the following areas within Customer Services:-

- Performance Management

- General and IT Contingency

3   Findings

3.1   The Customer Services Team deal with on average 3,269 calls per week, 169,988 per year and have face to face contact with 3,057 customers per week, 158,967 per year. The Service uses a Customer Records Management System to record data and use as a tool to deliver their service. This software is due to be updated next year.

3.2   The council have a number of policies which aid in creating an internal control framework. Internal Audit reviewed the Council's Document Retention Policy, Data Quality Policy and ICT Security Policies to ensure that they are current. Testing found that two of the policies did not include a review date, and therefore for best practice the owners of these documents should review the policies to ensure that they are still current.

3.3   The type of document will dictate how it is to be circulated. There is no formal written process for introducing new policies, employees are informed usually by email or through the staff news section on the intranet and then the policy/document is placed in its appropriate place, for example under documents or in the staff handbook both of which are located on the council's intranet site. New staff sign the council's ICT Security Policy on commencement of employment. Internal Audit asked a sample of staff if they are aware of the location of the above policies, testing found that in all but one member of staff were aware where they are located.

3.4   The Customer Services Team obtain personal data for a number of services, including; Planning Enquiries, Building Control Enquiries, Housing Enquiries, Pest and Dog Control Enquiries, Waste Management Enquiries, Land Charges Searches, Payments for the above services, Emergency calls, General Enquiries and Car Parks.

3.5   The Customer Services Manager has produced a Customer Service Centre Operating Protocol. Internal Audit was shown through the process for entering information onto their CRM system for the individual services mentioned above. Internal Audit was satisfied that the controls in place help to prevent duplicate or inaccurate information from being collected and used. Testing on a sample of information processed onto the CRM system found that it was accurate and correct.

3.6   All data collated by the Customer Service's Team is held electronically. All telephone calls are recorded and as per the Services Retention Policy deleted after 6 months. The CRM system does not have the facility to archive customer records, the Customer Services Manager informed Internal Audit that when possible the service will review inactive or possible duplicate accounts and mark them as "Do Not Use". Internal Audit has advised that as part of the upgrade the service needs to evaluate their CRM system to include an archiving facility.

3.7   The council have a number of IT drives to save their work and personal data. New staff are informed of the use of these drives at the council's Corporate Induction training sessions. Council staff are also informed through Team Briefs that are

published on the council's intranet. Testing found that some staff are not using the IT drives as specified. It has been agreed with the IT Operations Manager that they will remind staff via the council's intranet that all departmental work must be saved on the S: drive and space is allocated to save personal information only on the H: drive.

3.8   The Information Commission is an enforcement body for the Data Protection Act and Freedom of Information Act which the Council have a requirement to comply with. This area has not been reviewed as it has recently been audited by the Senior Auditor.

3.9   The service has processes in place in the event of the CRM system failing or complete IT failure. Also, in the event of the CRM system failing, the service have bought into a 'Council Local Information Online (CLIO) IT system. This is purely an information system that links into the council's website.

3.10   The maintenance of the CRM system is the responsibility of the councils Applications IT service. Internal Audit has been informed that for the continuity of service a member of their staff has been undertaking intensive training as a result of the Applications Support Analyst leaving the service at the end of February 2014.

3.11   Patches maybe required on systems used throughout the council to correct a fault or update the data infrastructure. Internal Audit was informed that no patches have been received from the supplier for the CRM application since its implementation in 2009. However, the Applications Support Analyst has carried out a test to ensure that systems across the council that use the CRM system are working correctly.

3.12   The council are required to comply with the government's code of connectivity. The council are tested externally to ensure compliance which includes undertaking an annual health check. Testing found that the council had passed the Public Service Network (PSN) compliance on 3rd September 2013. The council have an appropriate back up cycle in place. Internal Audit were informed that daily backups are undertaken and stored securely on site and weekly back-ups are taken and kept securely off site to enable recovery in the event of lost data. A record is kept of when these back-ups are undertaken, including those files that did not back up fully. Although the system has not been fully tested, when individuals have lost data the service has been able to recover the lost data.

4   Conclusion

4.1   Overall from the testing carried out, Internal Audit is satisfied with the records management of the Customer Service Centre. Internal Audit has made one low risk recommendation to strengthen the control in place. The implementation details of this recommendation can be seen in the Action Plan below.

5   Action Plan

	Recommendation	Officer	Priority	Agreed?	Comments	Implementation Date
3.2	Owners of the above policies ensure that the information within the policies is current and correct and that review dates and the individual who has undertaken the updates is entered to ensure a complete audit trail.	Head of Service Business Improvement	Low	Yes		With Immediate Effect.

High = Fundamental System Weakness – Action is Essential

Medium = Potential Control Weakness – Action Required

Low = Advised for Best Practice