Causeway Coast and Glens Borough Council

Internal Audit Report
Information Governance and Data Protection

November 2016
Final v2

MOORE STEPHENS

INTERNAL AUDIT REPORT

Information Governance & Data Protection

Executive Summary

This internal audit was completed in accordance with the approved annual Internal Audit Plan for 2016/17. This report summarises the findings arising from a review of information governance and data protection which was allocated 8 days.

Through our audit we found the following examples of good practice:

- An Information Security and Management Group has been established to lead on the development of policies and procedures relating to information governance and data protection and ensure consistency between policies (eg ICT policies and records management policies)
- Access to HR records was controlled, with legacy HR records securely locked at each of the 4 main Council sites
- A Data Protection Policy has been approved by Council.

Some areas where controls could be enhanced were noted during our review:

Priority 1

- A number of policies and procedures relating to information governance and data protection are currently in draft and the draft documents contain significant levels of information and detail. In addition, no formal training in data protection or information management has been provided since 1 April 2015. Within the legacy Councils, data protection training was only covered by one Council during induction (no ongoing data protection training for staff). There is a risk therefore that staff may not be aware of their responsibilities or the procedures required in relation to information governance and data protection which may lead to inadvertent actions that are not in compliance with the Data Protection Act 1998.
- We observed from a walk around of the 4 main Council sites a number of issues regarding information security; in particular, the strong room in Limavady containing archive files is left open all day and is not within sight of other offices or staff, a safe and filing cabinet containing papers used by Registration in Limavady were kept unlocked within the strong room during the day and a file containing copies of drivers' licences and insurance details was left in an open cabinet in an office in Ballycastle. There is a risk that the public as well as unauthorised staff could access the strong room in Limavady and staff not authorised to access the drivers' licence data could access the office in Ballycastle.

Priority 2

- An audit has commenced of all staff driving Council vehicles or driving their own vehicles but claiming mileage expenses. An external company is being used to

facilitate the audit and staff are required to produce copies of their drivers' licences and insurance certificates to their line managers for review. It is not clear that line managers have been provided with any guidance in relation to the data protection requirements for the information they will collect.

- We observed and noted from discussions that it can be difficult to identify staff as many staff are working in different sites and staff have merged from four legacy organisations. There is no consistency as to whether staff wear ID badges and we also observed that procedures for visitor sign-in are not consistent (with some offices not requiring visitors to sign in) and that visitor or contractor ID badges are not issued
- We were advised that the Premises Manager has tried to determine who the keyholders are for the main Council offices but that he has not been able to identify these definitively.

The following table summarises the total number of findings/recommendations from our audit (all recommendations being accepted by management):

Risk	Number of recommendations & Priority rating		
	1	2	3
The Council may not have an adequate governance framework covering information management and data protection leading to a lack of accountability for information management, increased risk of mismanagement of information and non-compliance with the Data Protection Act	1	-	-
The Council may not have adequate information retention measures in place leading to unauthorised storage and access to information	1	3	3
Information may be shared with external third parties without appropriate permissions leading to potential breaches of the Data Protection Act and regulatory action taken against the Council	-	-	1
The Council may not have appropriate archiving and information disposal arrangements in place leading to information being held for longer than is required or disposed of in ways that are not secure	-	-	2
Total recommendations made	**2**	**3**	**6**

Based on our audit testing we are able to provide the following overall level of assurance:

Limited	There are significant weaknesses within the governance, risk management and control framework which, if not addressed, could lead to the system objectives not being achieved

Points for the attention of Management

In addition to the recommendations noted above we have identified 3 system enhancements during the course of the audit which do not form part of our formal

findings, but may help enhance the existing controls. These are detailed at Appendix III.

Table of Contents

Auditor:	Camille McDermott / Steven Lindsay
Distribution:	Chief Executive Director of Performance Head of Performance Head of Policy and Community Planning Audit Committee November 2016

Audit progress	Date
Audit commenced	22/8/16
Draft Report issued to senior management for response	5/9/16
Responses Received	23/11/16 & 6/12/16
Responses Agreed	24/11/16 & 6/12/16
Report Issued	6/12/16

All matters contained in this report came to our attention while conducting normal internal audit work. Whilst we are able to provide an overall level of assurance based on our audit work, unlike a special investigation, this work will not necessarily reveal every issue that may exist in the Council's internal control system.

1 Objective

The areas for inclusion in the scope of the audit were determined through discussion with the Head of Policy and Community Planning. The scope of this audit was to review the arrangements in place within the Council in relation to information governance and data protection, focusing on the main risks associated with:

- Policies and procedures
- Training
- Data classification
- Information retention and security of data
- Data sharing.

Testing with regard to ICT controls in relation to access and security will be completed separately as part of the ICT Environment audit later in 2016.

2 Background

Information represents a significant asset for the Council and as such must be well managed. The Data Protection Act 1998 gives the public a right of access to information held about themselves and sets out a number of obligations that organisations holding personal data must adhere to. Under the Act, personal data is defined as:

> *data which relate to a living individual who can be identified –*
> *(a) from those data, or*
> *(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,*
> *and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.*

Sensitive personal data consists of information relating to:

> *(a) the racial or ethnic origin of the data subject,*
> *(b) his/her political opinions,*
> *(c) his/her religious beliefs or other beliefs of a similar nature,*
> *(d) whether he/she is a member of a trade union,*
> *(e) his/her physical or mental health or condition,*
> *(f) his/her sexual life,*
> *(g) the commission or alleged commission by him/her of any offence, or*
> *(h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.*

The Council holds a range of information about its staff (eg payroll and personnel records), the residents and members of the public with whom it engages (eg for Building

Control and Planning applications). The Council may also be required by law to collect and use information in order to comply with government requirements. All personal information must therefore be processed correctly in accordance with the Data Protection Act, including the collection, recording, using and storing of the information.

Information Governance relates to the management of the creation, classification, retention, transmission, and destruction of information.

3 Risks

The risks identified by Internal Audit relating to information governance and data protection and agreed with management are as follows:

1. The Council may not have an adequate governance framework covering information management and data protection leading to a lack of accountability for information management, increased risk of mismanagement of information and non-compliance with the Data Protection Act
2. The Council may not have adequate information retention measures in place leading to unauthorised storage and access to information
3. Information may be shared with external third parties without appropriate permissions leading to potential breaches of the Data Protection Act and regulatory action taken against the Council
4. The Council may not have appropriate archiving and information disposal arrangements in place leading to information being held for longer than is required or disposed of in ways that are not secure.

4 Audit Approach

Our audit fieldwork comprised:

- Documenting the systems via discussions with key staff
- Consideration of the key risks within each audit area
- Examining relevant documentation
- Carrying out a preliminary evaluation of the arrangements and controls in operation generally within the Council and reviewing controls within sample service areas (Environmental Health and Coleraine Leisure Centre)
- Testing the key arrangements and controls
- Testing the completeness and accuracy of records.

The table below shows the staff consulted with and we would like to thank them for their assistance and co-operation.

Job title
Head of Policy and Community Planning
Head of Health and Built Environment
Head of Performance

Job title
Head of Policy, Organisational Development and HR
Information Governance Officer
Premises Manager
Caretakers at each of the 4 main Council offices
Health Matters Fitness Instructor, Coleraine Leisure Centre

5 Findings and Recommendations

This section of the report sets out our findings in relation to control issues identified and recommendations. A summary of all the key controls that we considered is included in Appendix II to this report.

5.1 Risk 1 – Governance Framework

Recommendation 1 – *Policies, Procedures and Training*

a) Observation-

A Data Protection Policy has been approved by Council. A number of other policies and procedures relating to information governance and data protection are currently in draft; these include:

- Guide to Physical, Document and IT Security
- Data Protection Subject Access Request Procedure Manual
- Data Protection – Guidance for Staff and Members to assist with compliance
- Data Protection in the Visitor Information Centre Environment
- Data Security Breach – Guidance and Management
- Document and Records Control Procedure
- Information Sharing Policy
- Information Security Policy
- Records Management Policy
- Records Management Staff Handbook
- Redaction Guidance
- Request for information – general staff procedures
- ICT policies and procedures covering Security Incidents, Third Party Access, Removal Media, Bring Your Own Device etc.

The above documents contain significant levels of information and detail.

Legacy policies and procedures continue to apply in the absence of new policies and procedures being adopted; however we were advised that legacy policy and procedure documents are not available on the intranet.

With regard to training, no formal training in data protection or information management has been provided since 1 April 2015. Within the legacy Councils, data protection training was only covered by one Council during induction.

The Information Governance Officer has however provided data protection training to 22 members of staff in the Leisure and Development Directorate following a data

	breach and representatives from the Information Commissioner's Office delivered a presentation to Directors and the majority of Heads of Service covering data protection, Freedom of Information and Environmental Information Regulations.
b)	**Implication-** Staff may not be aware of their responsibilities or the procedures required in relation to information governance and data protection which may lead to inadvertent actions that are not in compliance with the Data Protection Act 1998. In addition, given the level of detail within the policies and procedures, there is a risk that staff will not read all the documents as they are implemented or may find it confusing since some are proposing procedures that are new to Council and the legacy Councils.
c)	**Priority Rating**- 1
d)	**Recommendation**- The various data protection and information management procedures (including ICT policies and procedures) should be finalised by the Information Governance Officer/Information Security and Management Group and implemented as soon as possible. There is a significant amount of detail in the various procedures and consideration should be given to reviewing how best to present this (eg creating simple flowcharts or shorter summary guides) to increase ease of understanding and likelihood of implementation. Given the number of procedure documents, the detail contained in them and the fact that data protection training will be new to many staff, training should also be delivered for staff covering the procedures as they roll out. Consideration should also be given to including information governance and data protection as part of formal staff induction programmes.
e)	**Management Response**- The majority of the documents in draft have now been approved by SMT, JCNC and Council and they will be put on the staff portal and Council website where appropriate. ICT policies and procedures have yet to be approved – responsibility of Head of ICT. The Information Governance Officer is currently preparing flow charts and summaries for these documents where appropriate. A training programme in relation to these policies and procedures, as well as general information governance issues, is currently being developed. The issue here is sourcing a trainer who can deliver this training at the various levels required. HR will be asked to consider the inclusion of information governance issues as part of the formal staff induction programmes.
f)	**Responsible Officer & Implementation Date-** Head of Policy Information Governance Officer OD/HR Flow Charts and Summaries prepared by January 2017 Training Programme in place by March 2017

5.2 Risk 2 – Information Retention and Security

Recommendation 2 – *File security*

a) Observation-

In general, files were securely locked in offices or document stores. However, we observed the following on a walk around each of the 4 main Council sites:

- A file labelled Driver Declarations (containing copies of drivers' licences and insurance details) was left in an open cabinet in an office in Ballycastle that had been used by Administration but was now being used by Leisure staff
- The strong room containing archive files in Limavady is kept open and unlocked all day and is not in sight of any staff or offices. Visitors to the Council's office in Limavady are also likely to pass by the room on the way to meetings or to use the toilet facilities
- A safe and filing cabinet containing papers used by Registration (such as certificates, paper for printing certificates, GRO stamps etc) in Limavady were kept unlocked within the strong room during the day
- Finance files labelled as relating to salaries and payslips (from 2008/09) were stored in the general archive shelves in the basement storage room in Coleraine accessible by all staff based in Coleraine and housing archives from all Council departments.

b) Implication-

There is a risk that unauthorised individuals could gain access to personal, sensitive or confidential information if it is not adequately secured.

c) Priority Rating-

1

d) Recommendation-

File security should be reviewed, particularly where staff are moving offices but leaving information behind, to ensure that no personal or confidential data is left unsecured.

In addition, the practice of leaving the strong room in Limavady unlocked and open during the day should be reviewed and the safe and filing cabinet used by Registration in Limavady should be locked at all times when not in use to prevent unauthorised access to Council files.

e) Management Response-

A process will be agreed within the Estates Strategy to ensure all information is secured when staff are moving offices

The Civic Facilities Manager will review the operation of the strong room in Limavady and put in place new secure arrangements.

f) Responsible Officer & Implementation Date-

Head of Corporate Performance and Compliance - December 2016
Civic Facilities Manager – December 2016

Recommendation 3 – *Information Classification*
a) Observation- An information classification system is proposed to be introduced in the draft Guide to Physical, Document and ICT Security. The classification system is based on that used by Government with the main classifications to be used being Official, Official-Sensitive and Official-Sensitive [Descriptor]. The use of these classifications will be a significant change for staff across the Council.
b) Implication- The guidance on the information classification is very detailed and, as the system is very different from processes used by Council currently, there is a risk that staff will be unsure of how to implement this.
c) Priority Rating- 3
d) Recommendation- Training and clear guidance should be provided to staff if the proposed information classification system is introduced. Consideration should also be given as to how to support staff in implementing the classification system and in monitoring that it is effectively supporting Council to understand the information that it holds and the level of security required to protect it.
e) Management Response- The Records Management Policy and the Records Management Handbook have both now been approved by SMT, JCNC and Council. Both have been placed on the staff portal. A training programme on the system to be provided when an appropriate trainer has been sourced. Implementation of a monitoring system will take place follow the roll out of the training for appropriate staff.
f) Responsible Officer & Implementation Date- Head of Policy Information Governance Officer OD/HR Training Programme in place by March 2017 Monitoring System by May 2017

Recommendation 4 – *Information Asset Registers*
a) Observation- It is good practice for organisations to understand the information assets that they hold. The draft Records Management Staff Handbook proposes that each department will be responsible for completing an Information Asset Register (template within the handbook) to identify the purpose, sensitivity and retention/destruction requirements for the information it holds. This procedure is likely to be new staff across Council
b) Implication- Staff may not understand what information should be recorded in the register or how best to undertake the exercise. The assessment of information assets may therefore not be completed.
c) Priority Rating- 3
d) Recommendation- Consideration should be given as to how to implement the creation of departmental information asset registers to ensure that staff are supported through the process and that adequate records of information assets are maintained.
e) Management Response- An Information Risk and Assurance process has been agreed by SMT, JCNC and Council. This involves the appointment of a Senior Information Risk Owner, Information Asset Owners and Local Information Co-Ordinators within Council. One of the responsibilities of the Information Asset Owners and Local Information Co-Ordinators is to maintain their Department's information asset register. These staff have yet to be identified and once in place a training programme will be rolled out to implement the process. The Information Governance Officer will provide on-going support thereafter.
f) Responsible Officer & Implementation Date- SMT Head of Policy Information Governance Officer OD/HR Relevant staff identified and trained by May 2017.

Recommendation 5 – *Driver Audit Details*
a) Observation- An audit has commenced of all staff driving Council vehicles or driving their own vehicles but claiming mileage expenses. An external company is being used to facilitate the audit and staff are required to produce copies of their drivers' licences and insurance certificates to their line managers for review. It is not clear that line managers have been provide with any guidance in relation to the data protection requirements for the information they will collect (which will be classed as personal under the Data Protection Act 1998 and potentially sensitive if driving convictions are also notified).
b) Implication- Line managers may not retain the copies of driver licences and insurance securely or may seek to record more information than is required for the purposes of the audit. Additionally, the Council may not have assurance that the external company being used will adequately protect the data it holds on each driver.
c) Priority Rating- 2
d) Recommendation- The Information Governance Officer should work with the Head of Performance to ensure that information that is collected as part of the driver audit (eg driver licence and car insurance details) is adequately protected and that no more information than is required is collected. If line managers (rather than a central unit) are to be tasked with collecting this information, guidance should be provided to all line managers as to what information to collect, how to store it and who it should and should not be shared with.
e) Management Response- The Information Governance Officer has recommended the following: • Centralising the review of licence details so that one person has overall responsibility rather than all line managers across Council. • Ensuring that officers collecting this information understands what they should/need to record, eg it may be sufficient to note information such as driver licence expiry date or that they've seen a valid insurance certificate rather than keeping copies of these documents. • Ensuring the person collecting the information understands the need to store personal information such as this securely. • Verifying how any external agency used to complete the audit will ensure the security of the data held – is this covered in the contract?
f) Responsible Officer & Implementation Date- Head of Corporate Performance and Compliance – January 2017

Recommendation 6 – *Keyholders*	
a)	**Observation**- We were advised that the Premises Manager has tried to determine who the keyholders are for the main Council offices but that he has not been able to identify these definitively. We were advised that costings for replacing the locks at the main Council sites has been included within the proposed Estates Strategy.
b)	**Implication-** There is a risk that staff who no longer work for the Council or who have moved into a different role may have retained keys and could therefore access premises without authorisation. Additionally, there is a risk of a lack of control over keys whilst the change management processes to merge the four legacy organisations continues.
c)	**Priority Rating**- 2
d)	**Recommendation**- The Premises Manager should continue to identify keyholders for the main Council sites. In the meantime and until the Estates Strategy has been fully implemented and access controls updated for each building, staff should be reminded to ensure that confidential, personal or sensitive information is kept secure at all times.
e)	**Management Response**- The premises key holder system will be reviewed to ensure appropriate control arrangements are in place. Reminder about keeping confidential, personal or sensitive information secure – e-mail from Director of Performance.
f)	**Responsible Officer & Implementation Date-** Head of Corporate Performance and Compliance – February 2017

Recommendation 7 – *Staff, Visitor and Contractor Identification*	
a)	**Observation**- Some staff have taken up the option of having ID badges and the facility to print and create the badges in-house (rather than being sent to an external supplier) has recently been acquired by the Premises Manager. We observed and noted from discussions that it can be difficult to identify staff as many staff are working in different sites and staff have merged from four legacy organisations. We also observed that procedures for visitor sign-in are not consistent (with some offices not requiring visitors to sign in) and that visitor or contractor ID badges are not issued.
b)	**Implication-** There is a risk that unauthorised individuals may gain access to areas that they should not be in and could therefore gain unauthorised access to sensitive or confidential information.
c)	**Priority Rating**- 2
d)	**Recommendation**- Council should roll out the ID badge system to all staff, visitors and contractors to ensure that people can be easily identified and that no unauthorised individuals gain access to information or areas which should be restricted.

e) Management Response-
The Council has recently purchased a machine to produce ID badges and a policy and process will be created to implement the changes.

f) Responsible Officer & Implementation Date-
Civic Facilities Manager – April 2017

Recommendation 8 – *Electronic information security*

a) Observation-
We noted from a review of projects that Environmental Health is involved in and one Leisure project that databases containing the details of participants in the project were stored in a Council staff member's personal drive in the network for 2 of the projects (Home Safety and Health Matters) and secured as the staff member's login is required to access the computer and therefore the personal drive. We noted however that a general database containing names, addresses and referral agencies for the Affordable Warmth scheme was stored in the shared Environmental Health drive and was not password protected. We were advised that the process of reviewing the departmental Environmental Health folders has commenced and this will be considered as part of that.

Given that ICT systems are still being merged and that staff may create databases themselves across the Council, it is likely that information may currently be within shared drives that should be given greater restriction.

b) Implication-
There is a risk that unauthorised staff may gain access to personal data held in databases.

c) Priority Rating-
3

d) Recommendation-
Managers should be advised to review whether databases that may be held within their departments holding personal details relating to projects (names/addresses etc) should be password protected or restricted folders set up so only those department staff working on the project can access the data.

e) Management Response-
E-mail can be circulated to this effect to staff by the Director of Performance

The Information Security and Management Group will be considering developing recommendations on password protecting documents when sending them through unsecure servers.

f) Responsible Officer & Implementation Date-

SMT/Heads of Service – March 2017

5.3 Risk 3 – Information Sharing

Recommendation 9 – *Information Sharing Protocols*
a) Observation- We selected a sample of projects that Council is involved in with other agencies (in Environmental Health and Leisure) and reviewed whether an information sharing protocol was in place or whether information sharing and management was covered under existing agreements or contracts. We found that of the 6 schemes considered, two had a specific information sharing protocol or mention of such within the project service level agreement (Landlord Registration scheme with NIHE). For others such as the Health Matters project and Home Safety Scheme, there did not appear to be a protocol in place to cover sharing of personal information from, for example, Health Trust staff referring individuals and families to Council projects. Additionally, where Council is engaged in joint projects with other Councils, such as the Animal Welfare Service, we did not identify any reference to information sharing and information ownership within the service level agreements. We also noted that these projects (except the Landlord Registration Scheme) are not recorded on the Data Sharing Agreement Register developed by the Information Governance Officer to track information sharing arrangements between Council and other organisations.
b) Implication- The responsibilities for collecting and storing information and the protocols regarding information ownership and information sharing may not be adequately defined. There is a risk therefore that information could be shared inappropriately or in a way that is not in accordance with the Data Protection Act 1998. Additionally, staff may be unclear as to when an information sharing protocol is required.
c) Priority Rating- 3
d) Recommendation- The Information Governance Officer should work with Managers to identify where Council is engaged in data sharing arrangements and review whether there is a need for information sharing protocols to be developed for projects in which personal data is shared between agencies, if no such protocol currently exists (particularly where this is shared on a systematic basis and if information sharing responsibilities and requirements are not set out within a project agreement or contract).
e) Management Response- The Information Governance Officer will work on a one to one basis with all Heads of Service to assist them in identifying where information sharing protocols already exist or need to be put in place.
f) Responsible Officer & Implementation Date- Information Governance Officer – on-going work.

5.4 Risk 4 – Information Disposal

Recommendation 10 – *Old Files*
a) Observation- On a walk around each of the four main Council offices and file stores / archives, we observed files dating from the 1990s and as far back as 1977. From those Heads of Service that we spoke with, information has not generally been disposed of since April 2015. The Council is currently awaiting approval of its Retention and Disposal Schedule by the NI Assembly. We also noted from our walk around that files and information remain on shelves / the floor / windowsills in offices that may have been vacated.
b) Implication- Organisations should not hold information for longer than necessary under the Data Protection Act 1998. Additionally, it is likely that Council will need to free up space to accommodate live / recent archive files as the Estates Strategy is implemented.
c) Priority Rating- 3
d) Recommendation- A process should be put in place to review the information held by Council (both hard copy documents in offices and archive/storage and electronic information) to dispose of information that is no longer required to be held. All records should be disposed of in accordance with the approved retention and disposal schedule.
e) Management Response- The Council's Retention and Disposal Schedule has now been approved by the Assembly and the Chief Executive has circulated an e-mail advising Heads of Service that the Schedule is now operational. A copy of the approved version was attached and managers advised that all records should now be disposed of in accordance with the Schedule. With regard to legacy records, these have now transferred to the responsible service area and should also be dealt with under the new Retention and Disposal Schedule. In addition, managers were advised by the Chief Executive that, in accordance with the Public Records Act (NI) 1923, a record of each file destroyed must be kept. An excel spreadsheet was attached for this purpose and a copy was to be updated at each Department / Directorate level. Relevant training will be delivered in due course on records management to include specific training for Local Information Co-Ordinators who will have responsibility for retention and disposal of records.
f) Responsible Officer & Implementation Date- All Heads of Service Local Information Co-Ordinators OD/HR On-going work.

Recommendation 11 – *Confidential Waste Collection*

a) Observation-

We reviewed the confidential waste disposal arrangements for each of the 4 main Council sites. Arrangements are currently operating under the legacy contracts although it is intended to tender for a new Council-wide contract. All confidential waste is collected and shredded by the contractor at each site, in the presence of a member of Council staff. Confidential waste collection practices however differ between the 4 sites, most particularly:

- There are no confidential waste bins for staff to dispose of confidential waste in Ballycastle. Staff retain their confidential waste by their desks until they have sufficient to request a confidential waste bag from the Caretaker
- Caretakers in Coleraine empty the confidential waste bins and store the bags until collection by the external disposal contractor. Caretakers in Ballymoney and Limavady do not open or empty the confidential waste bins as this is carried out by the contractors directly
- Confidential waste bags are generally stored securely prior to collection by the contractor. Bags in Ballycastle are stored in a locked store that is shared with Development staff and we observed that a confidential waste bag in the store had not been sealed.
- The filing of signed confidential waste collection notes differed with some being held by Recycling Officers and others by Caretaking staff. The collection notes for Ballycastle could not be located during our audit.

We also tested the collection notes, where available, for the last year and found that all had been signed by a Council representative to evidence witnessing the document shredding, except for 1 of the 7 Ballymoney collection notes reviewed and 2 of the 5 Limavady collection notes reviewed. We were also advised that on occasion, confidential waste is shredded on site by the contractor in Limavady without a Council member of staff present if the Caretaker or Recycling Officer are not available.

b) Implication-

Confidential waste may not be adequately secured prior to disposal. Additionally, there is a risk that confidential waste might not be shredded if not witnessed by a member of Council staff.

c) Priority Rating-

3

d) Recommendation-

A consistent process for the disposal and collection of confidential waste should be implemented across the Council's sites including access to confidential waste bins for all relevant premises, shredders if required and defined procedures for storage of confidential waste, review and filing of signed collection notes/certificates of destruction. Staff should be provided with guidance as to the confidential waste arrangements at their site and what should and should not be placed in the confidential waste.

Staff should also be reminded to ensure that they sign the confidential waste collection notes as evidence that they observed the waste being shredded.

e) Management Response-

Agreed.

f) Responsible Officer & Implementation Date-
Civic Facilities Manager - April 2017. Start with civic facilities and then Business Support managers to lead in Environmental Services and Leisure and Development.

Appendix I: Definition of Assurance Ratings and Hierarchy of Findings

Satisfactory Assurance
Evaluation opinion: Overall there is a satisfactory system of governance, risk management and control. While there may be some residual risk identified this should not significantly impact on the achievement of system objectives.

Limited Assurance
Evaluation opinion: There are significant weaknesses within the governance, risk management and control framework which, if not addressed, could lead to the system objectives not being achieved.

Unacceptable Assurance
Evaluation opinion: The system of governance, risk management and control has failed or there is a real and substantial risk that the system will fail to meet its objectives.

Hierarchy of Findings

This audit report records only the main findings. As a guide to management and to reflect current thinking on risk management we have categorised our recommendations according to the perceived level of risk. The categories are as follows:

Priority 1: Failure to implement the recommendation is likely to result in a major failure of a key organisational objective, significant damage to the reputation of the organisation or the misuse of public funds.

Priority 2: Failure to implement the recommendation could result in the failure of an important organisational objective or could have some impact on a key organisational objective.

Priority 3: Failure to implement the recommendation could lead to an increased risk exposure.

Appendix II: Summary of Key Controls Reviewed

Information Governance and Data Protection

Risk	Key controls
The Council may not have an adequate governance framework covering information management and data protection leading to a lack of accountability for information management, increased risk of mismanagement of information and non-compliance with the Data Protection Act	• A proposal on an information assurance strategy has been developed and key information risks have been identified • The roles and responsibilities for information management are defined in draft procedural documents – subject to audit recommendation • There is an adequate Data Protection Policy in place • Staff and elected members have been made aware of the Data Protection Policy • Processes have commenced in some areas to ensure that personal data held remains factually correct and relevant • The Council has a draft policy covering disclosures or sharing of personal data with third parties – subject to audit recommendation • Staff have received training in information management and data protection - subject to audit recommendation • Staff are given guidance on how to transmit either personal or sensitive hard copy and electronic information to external sources – subject to audit recommendation (currently within draft procedures)
The Council may not have adequate information retention measures in place leading to unauthorised storage and access to information	• Council has developed an information classification scheme – subject to audit recommendation • Council has a record of the information it holds including ownership, purpose, sensitivity and retention/destruction requirements – subject to audit recommendation • A records management system is in place – subject to audit recommendation • Council has a draft information security policy • Physical access controls are applied to manual records - – subject to audit recommendation • Staff are given guidance on what devices (eg laptops, external hard drives, USB pens) they should use to store electronic information in draft ICT policies • The Council has defined procedures for dealing with information security incidents (currently in draft) • Information security incidents are appropriately reported to management and to the Information Commissioner if required
Information may be shared with external third parties without appropriate permissions leading to potential breaches of the Data Protection Act and regulatory action taken against the Council	• Council has an information sharing policy (currently in draft) • Staff are given guidance on how to transmit either personal or sensitive information (hard copy and electronic) to external sources (currently in draft) – subject to audit recommendation • Staff are given guidance on the security precautions that must be taken when taking information (either hard copy

Risk	Key controls
	or electronic) off site (currently in draft) – subject to audit recommendation • Authorisation is received by the information owner before the information is transmitted to an external source • Council has signed information sharing protocols with relevant external third parties (eg NILGOSC for payroll data and DOE for Planning information) – subject to audit recommendation • Sensitive information transmitted in electronic or hard copy outside of the organisation is adequately protected (eg by encryption) – subject to audit recommendation
The Council may not have appropriate archiving and information disposal arrangements in place leading to information being held for longer than is required or disposed of in ways that are not secure	• Document retention policy has been developed and communicated to staff (currently awaiting NI Assembly approval) • Council has appropriate archive arrangements – subject to audit recommendation • Archives are secure and can only be accessed by those authorised to do so – subject to audit recommendation • The disposal and destruction of sensitive information is carefully managed – subject to audit recommendation

Appendix III: Points for the Attention of Management

Risk Assurance Roles and Responsibilities
A proposal has been made to establish formal information governance roles, including Senior Information Risk Owners, Information Asset Owners and Information Coordinators. If implemented, it is important those undertaking these roles are clear as to the requirements of the role and consideration should be given to providing specific training for the staff who will take on these roles.
Management response: An Information Risk and Assurance process has been agreed by SMT, JCNC and Council. This involves the appointment of a Senior Information Risk Owner, Information Asset Owners and Local Information Co-Ordinators within Council. One of the responsibilities of the Information Asset Owners and Local Information Co-Ordinators will be the maintenance of their Department's information asset register. These staff have yet to be fully identified. Once in place a training programme will be rolled out to implement the process (by May 2017). The Information Governance Officer will provide on-going support thereafter.

Data Security Breach – Guidance and Management
The draft Data Security Breach – Guidance and Management document does not make reference to the data security breach register established by the Information Governance Officer. In addition, the draft document contains guidance from a law firm as an appendix which may confuse staff as to which procedures to follow. Consideration should therefore be given to whether to include the guidance within the appendix of the data security breach procedures. It is important that the step-by-step instructions for how to deal with breaches are set out within the procedures and the procedures should also reference the data security breach register and the responsibility for maintaining this register, as well as the role of the Information Governance staff in dealing with any breach.
Management response: The draft Data Security Breach – Guidance and Management document has been amended in light of these comments and has now been formally approved by Council (via the Corporate Policy and Resources Committee).

Version Control Guidance
A draft Document and Record Control Procedure (Version Control) has been prepared. The same guidance is also included in the Records Management Staff Handbook. Consideration should therefore be given as to whether there is a need for a separate version control procedure.
Management response: The separate version control procedure has been withdrawn and the Records Management Staff Handbook contains guidance on version control.