1. PURPOSE:

To update members of the Audit committee with regard to the information governance, strategy and procedures in MCC.

2. RECOMMENDATIONS:

That Audit Committee consider the content of the report.

3. KEY ISSUES:

3.1 Background and context of information management in MCC

3.1.1 Information is a key resource of any organisation, and if it isn’t accessible to the right person, at the right time and in the right place can have the following effects –

- Service disruption when key information is not available to provide the service
- Financial and reputational loss if gets into the wrong hands
- Poor decision making when using inaccurate information

3.1.2 It is essential that information, whether in digital or physical format, is protected but accessible and MCC has policies and practices in place to ensure this is the case. Physical storage can be destroyed by fire/water or accidentally disposed of by employees. This can cause business continuity problems. More and more data is being stored digitally in MCC and it is essential to protect this resource.

3.1.3 With mobile digital data on the increase it is essential that security goes hand in hand with the devices used to store and retrieve it. These mobile devices are desirable in themselves, but more importantly they allow access to potentially sensitive information stored on the device itself as well as on e-mails. More importantly, they could provide a potential gateway to personal and sensitive information stored in the network data storage within the organisation.

3.1.4 It is imperative that data is secure but accessible, and these two features sometimes contradict each other. It is important to balance the risk of data loss against the need to run the business efficiently and effectively.

3.1.5 MCC recognises the importance of information governance, and through its’ SIRO, Information Manager and Data Protection Officer ensures that its’ information security responsibilities are discharged.
3.2 MCC Information Governance Arrangements

3.2.1 MCC has an information strategy and policy in place, which is backed up with training and procedural guidance. It is important to note that information management is the responsibility of EVERY employee and Member of the council. It is a thread that runs through the organisation in the same way as ICT, Finance and HR. It isn’t the sole responsibility of one or two individuals in the information management team. To date MCC hasn’t had any recordable data breaches, and it is essential to ensure that the introduction of the iCounty strategy and the increase of digital data that digital security is the main focus for security.

3.2.2 Though ICT enables information to be stored and retrieved efficiently, effectively and securely the council considers that information governance/management is not an ICT issue and has chosen to separate the governance arrangements from the ICT service. The council’s SIRO is the Head of Democracy and Regulatory Service. Information is managed at a strategic level by the Information Manager and is delivered through a network of information champions within each service area.

3.2.3 MCC has governance arrangements for the operational management of information. These include:

- The Information Governance Group – A selection of reps from service areas to discuss procedures, inform policy and define training requirements.
- Information Assurance Governance Board – A specific ICT information security group with reps from Gwent Police TCBC SRS and MCC. Its main function is to ensure we comply with the various government and legislative protocols, including the PSN Code of Connection.

3.2.4 Effective information management starts with strategy and policy, but in order to embed it through the council it relies upon employees being trained and updated on information security issues. In Monmouthshire this includes the following -

- Staff and Members undergo data protection and information management training on induction and through regular training events. Training has also been extended out to schools as requested.
- An information audit was carried out in each service as part of the introduction of Agile Working 4 years ago. Each service received a report on the information retention requirements in order for them to manage their data retention in line with the DPA.
- SharePoint is being developed as the council’s EDRMS with Team sites being developed for each service to access information in one place with security levels ensuring that information is accessible yet safe. This also ensures that we maintain ‘one version of the truth’ i.e. that there is only one current version of a document. SharePoint is also the platform for the council’s intranet site ‘Hub’ and is the storage point for corporate documents with search facilities across the network drives.
- MCC now have an agreed and updated Business Continuity Policy in place and Simon Burch (corporate director of SC&H) has been appointed as the MCC Business Continuity Management (BCM) Champion. A Register of Critical Services has now been compiled and each system allocated a priority rating in order that information is available in the event that business is severely disrupted for whatever reason.
The council's ICT strategy called i-County was implemented in June 2014. This strategy sets the direction of ICT. The information strategy sits alongside the i-County strategy in delivering secure ICT services.

Specific ICT related security is supplied by a data security team at the SRS (Shared Resources Service). This team monitors security of applications and devices as well as the infrastructure and networks used by the Council. Compliance with the Code of Connection is also undertaken by this team.

3.2.5 The Wales Audit office has undertaken several reviews of information management arrangements as follow and any proposals for improvement have been reported to the committee and action taken to address.

- Information Management Themed Review April 2012
- Technology Themed review reported Oct 2011
- Proposals for Improvement Follow up Aug 2012 and updated June 2014

4. REASONS:

4.1 Information is a valuable resource to MCC, and if it is inaccurate or lost can cause businesses continuity problems, poor decision making and inefficiency in service delivery. It is essential that information is controlled yet accessible to the right person at the right time. Audit committee need to be satisfied that the information governance arrangements on place are robust and appropriate to the organisation.

5. RESOURCE IMPLICATIONS:

There are no resource implications as a result of this report.

6. BACKGROUND PAPERS:

Information Policy

Information Strategy

7. AUTHOR: Sian Hayward, Digital and Technology Manager

8. CONTACT DETAILS:

Tel: 07971893998
E-mail: sianhayward@monmouthshire.gov.uk