RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

MUNICIPAL YEAR 2017-18

OVERVIEW & SCRUTINY COMMITTEE
14TH NOVEMBER, 2017

REPORT OF THE HEAD OF ICT

AGENDA ITEM No. 4

INFORMATION MANAGEMENT (IM) FUNCTION/GOVERNANCE ARRANGEMENTS AS PART OF THE ANNUAL WORK AND PERFORMANCE UPDATE.

1. PURPOSE OF THE REPORT

1.1 To provide Overview & Scrutiny Committee members with an overview of the Information Management (IM) function / governance arrangements as part of the annual work and performance update.

2. RECOMMENDATIONS

2.1 It is recommended that Members:

i. Acknowledge the remit of the IM function and the potential risks of non compliance with associated legislation and standards in particular the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR).

ii. Acknowledge the Councils Information Governance structure and reporting arrangements.

iii. Form a view on the adequacy of arrangements in place to monitor and review the Council's work and performance for managing data

iv. Agree to receive a periodic report from the Senior Information Risk Owner (SIRO) on the Councils work and performance around Information Management.

v. Propose and agree the scope, criteria, frequency and reporting arrangements in respect of recommendation iv.

3. BACKGROUND & CONTEXT

3.1 At the Audit Committee on the 5th June 2017 the Service Director – Performance and Improvement presented Members with the Council's draft Annual Governance Statement for the 2016/17 financial year that aims to provide an accurate representation of the governance arrangements in place for financial year ending 31st March 2017.

3.2 The draft statement (Point 5.8) outlines the arrangements in place for managing risk and performance through robust internal controls and strong financial management with the 'management of data' being a key component.

3.3 The statement also highlighted that no arrangements were noted that set out, on a periodic basis, the Council's work and performance for managing data.

3.4 The following action for improvement was proposed:

''The Council should report on a periodic basis, for example annually, its work and performance around Information Management and provide opportunity for review and scrutiny''.

3.5 It was requested at the meeting that the report on the Council's work and performance around Information Management is referred to the Overview & Scrutiny Committee for consideration. The Service Director, Performance and Improvement confirmed that arrangements will be made for this 'topic' to be incorporated onto the draft 2017/18 work programme for the Overview and Scrutiny Committee.

4. DEFINITION OF INFORMATION MANAGEMENT

4.1 Information is a key asset for the Council. It is central to the Council's business processes, decision making and service delivery. It also provides evidence and ensures accountability for Council actions and performance. It is crucial that information is managed effectively to maximise value for the Council, its citizens, and to manage related risks.

4.2 Information Management provides a framework that brings together all of the legal and regulatory requirements, standards and best practice in relation to data quality, information compliance, information security, information sharing and records management. Overall, it ensures that the Council is creating, managing, using, sharing and disposing of information efficiently, appropriately and lawfully.

4.3 The Council holds and processes huge volumes of personal and sensitive information which is necessary for the efficient and effective delivery of services. Consequently, and recognising the size and diversity of the Council, an information management framework that is flexible and responsive to changes in risks and to services delivered is essential.

4.4 The Council is committed to preserving the confidentiality, integrity and availability of all its physical and electronic information systems and records in order to provide assurance that the Council manages its information risks:

- So that the needs of service users and citizens and the requirements of corporate governance are met;
- To establish confidence that partnership arrangements involving sharing and exchange of information are legal and secure;
- To establish that designed and implemented security features are effective;
- To provide confidence that services and products offered by third parties manage information risks on behalf of the Council in a way which is adequate and fit for purpose.

5. LEGAL DRIVERS

5.1 The effective management of information places significant demands on the Council. In particular, there is a wide ranging, dynamic and complex legal landscape in which the Council has to operate within.

5.2 The following details the principal acts, regulations, and technical standards concerning information governance which the IM function seeks to align, achieve and maintain compliance with:

- Data Protection Act 1998 (DPA) – to be replaced by the General Data Protection Regulation (GDPR) wef May 2018
- Freedom of Information Act 2000 (FOI)
- Environmental Information Regulations 2004 (EIR)
- Privacy and Electronic Communications Regulations
- Regulation of Investigatory Powers Act 2000 (RIPA)
- The Public Services Network Code of Connectivity (PSN)
- Information Security Management Systems – e.g. ISO/IEC 27001:2013
- Local Public Services Data Handling Guidelines (Fourth Edition – February 2017)
- Welsh Governments 'Wales Accord on the Sharing of Personal Information (WASPI)' framework

6. ENFORCEMENT ACTION

6.1 Failure to manage information appropriately can lead to reputational loss and considerable financial penalties. In particular, the Information Commissioner's Office (ICO) has a wide range of enforcement powers to change the behaviour of organisations who are found to breach the Data Protection Act (DPA). The enforcement powers include but are not limited to:

- **Monetary penalty notices** of up to £500,000 for each breach under the DPA (UK legislation.
- This will increase to the following under the GDPR, when it comes into force in May 2018:
  - Tier 1: Up to €10M or 2% organisations global turnover – for organisational non compliance (failing to keep records of processing activities, undertake privacy impact assessments (PIA), appoint a Data Protection Officer).
  - Tier 2: Up to €20M or 4% organisations global turnover – for breaches of the data protection principles (data loss / theft, inappropriate disclosure etc.).
- **Serve enforcement notices** (and 'stop now' orders) - where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law.
- **Serve assessment notices** to conduct compulsory audits to assess whether organisations' processing of personal data follows good practice.

7. INFORMATION GOVERNANCE STRUCTURE / ARRANGEMENTS

7.1 The Head of ICT has specific responsibility for Data Protection, ICT Security and the delivery of IM priorities as contained within the ICT Service Delivery Plan. The Head of ICT is supported by the IM & Security Management Team.

7.2 Specific roles, responsibilities and governance arrangements have also been established in line with the Local Public Services Data Handling Guidelines and WAO recommendations.

7.3 The following IM governance structure is in place within the Council.

7.4 Senior Information Risk Owner (SIRO)

7.5 The Group Director Corporate and Frontline Services is the designated SIRO for the Council.

7.6 The SIRO is a key role in ensuring that there are robust systems and processes in place to safeguard our information assets and that any risk associated with information is appropriately managed. Some of the key responsibilities of the Senior Information Risk Owner are:

- to foster a culture for protecting and using information within the Council
- the development of the information management strategy/plan
- to ensure information governance compliance with legislation and Council policies
- to provide a focal point for managing information risks and incidents

7.7 Information Asset Owners

7.8 The SIRO is supported by Information Asset Owners (IAO). The role of the IAO is at senior level (typically Head of Service), assigned to Officers who have ultimate ownership and accountability of information systems and assets held within their service area. The IAO has responsibility for making sure that information systems and assets are handled and managed appropriately. This means making sure that information is properly protected, and where personal information is shared, that proper confidentiality, integrity and safeguards apply.

7.9 Information Management Board

7.10 The IM Board provides high level oversight and support to the SIRO. It determines the long term information management plan for the Council, monitors progress against the plan and provides assurance that information risk is being properly assessed, controlled and mitigated.

7.11 The Board is chaired by the SIRO and permanent group members consists of:

- Head of ICT
- Head of Legal – Corporate & Democratic Services
- Head of Organisational Development
- Operational Audit Manager
- ICT Programme & Support Manager
- Principal Information Management & Data Protection Officer

7.12 Information Management Working Group

7.13 The group supports the delivery of the information management plan, and is responsible for operationally supporting, monitoring and learning from information security incident investigations and raising awareness of IM and DP within their Service Group.

7.14 The group is attended by key service representatives whose role is to provide a first point of contact for staff and managers for advice and information on information management related issues such as data protection, information security and information sharing within their service.

8. INFORMATION MANAGEMENT PRIORITIES

8.1 IM priorities form part of the ICT Service Delivery Plan and are based around the following key aims that are designed to support the continual improvement of performance for managing data :

a) Develop/communicate clear IM policies and procedures

To develop & communicate clear policies for access to information, data protection, records and document management, information sharing and information security. Policies will deal with issues of complaints, consistency, use of information in relation to Council priorities and privacy.

b) Changing the culture through communication and training

Training, education and awareness are essential to ensure compliance with policies and procedures, as well as promoting a culture of corporate responsibility that values information as an asset.

Specific training requirements identified through an information risk management approach will be delivered at an appropriate level to all staff over a period of time, using existing training and communication mechanisms such as e-learning.

c) Compliance, monitoring and reporting

Set targets that are aligned with the overarching corporate priorities alongside requirements for compliance with legislation and security accreditation.

9. INFORMATION MANAGEMENT MONITORING ARRANGEMENTS

9.1 The Council's IM arrangements are monitored on a quarterly basis by the IM Board in the form of a highlight report, and locally by service champions.

9.2 The highlight report provides a position statement/summary of the following:

a) Progress of IM priorities against the ICT Service Delivery Plan

b) Information security incidents and events (call volumes, call type, lessons learned/improvements etc.)

c) Information security incidents reported to the Information Commissioner's Office.

d) Subject Access Requests (SAR) received and responded to within the statutory time period.

e) Freedom of Information requests received and responded to within the statutory time period (to be incorporated within report wef Qtr. 2 17/18).

10. WALES AUDIT OFFICE (WAO) REVIEW

10.1 The Council's Information Management arrangements are scrutinised by the WAO.

10.2 In 2010 the WAO identified that many local authorities were grappling with using information effectively to support service transformation and efficiency savings. As a result, reviews of information management were undertaken at all Councils in Wales. These reviews sought to answer the question: 'Is the Council's approach to information management positively supporting improvement?'

10.3 The WAO carried out an initial review of the Council in September 2011 and reported their findings in February 2012. The report proposed six key areas for improvement and concluded that:

"The Council has focused on the governance and management of electronic information and has not yet fully addressed the issues and risks associated with paper information; when strengthened and broadened to cover the entire information asset the arrangements have the potential to support improvement."

10.4 In January 2013, the WAO reviewed the Council's progress in implementing the six proposals for improvement arising from the February 2012 review. The WAO found that:

"Progress has been made on all six proposals for improvement, strengthening and broadening the Council's arrangements for the governance and management of its information asset."

10.5 In 2016 the WAO undertook a further risk based assessment of the Council's corporate arrangements in particular focusing on Information & Communications Technology and Information Governance. The WAO reported their findings in a letter to the Chief Executive on the 24th August 2016 and noted the following in relating to the Council's information governance arrangements:

''The Council has generally sound information governance arrangements and is making steady progress to improve its management of information. Few changes have been made to established governance arrangements since the previous Head of Customer Services and ICT left the Council earlier this year. However, the role of Senior Information Risk Owner (SIRO) has now transferred to the Group Director for Corporate and Frontline Services. The Council has indicated that it intends to further review its information governance arrangements over the coming months. In the meantime, we are satisfied that the current arrangements are appropriate to ensure that the Council complies with its legislative responsibilities''.