Audit & Governance Committee

Date of Meeting: 30 July 2019

Report Title: Annual Information Governance Update 2018/19

Senior Officer: Frank Jordan, Executive Director – Place

1. Report Summary

1.1. This report provides an update on the Council's Information Assurance and Data Management (IADM) programme.

2. Recommendation/s

2.1. That the Committee note the progress made on the Information Assurance Programme during 2018/19.

3. Reasons for Recommendation

3.1. To provide the Audit and Governance Committee with an update on Information Assurance.

4. Other Options Considered

4.1. Not applicable.

5. Background

5.1. There is a rising expectation that public authorities handle information on behalf of its citizens in a robust manner. Protecting people's personal information ranks in the top 10 concerns in a survey by the Information Commissioner's Office. A data protection law expert from Pinsent Masons stated recently that "*organisations need to ensure that they not only have appropriate policies and procedures in place but that they can demonstrate through risk assessment, audit and review that that the processes being adopted meet the standards of the GDPR and the UK's new Data Protection Act of 2018. Essentially, the culture of compliance should be within the DNA of the business*".

5.2. The General Data Protection Regulation (GDPR) places data protection privacy by design and by default at its heart, meaning that organisations need to integrate data protection into their data processing activities and business practices. GDPR also sets out the principles that organisations need to follow and the penalties to be expected should they not comply. Penalties for non-compliance for the Council can now be up to €20 million.

5.3. Public Sector organisations are also expected to comply with the Government's Transparency Agenda and publish information so that it is readily available i.e. open data. The underlying principle for open data is that Government will be more accountable by publishing information to the public and consequently engender greater trust from its citizens. The two positions of being open and at the same time secure may seem at odds, one to protect, one to share but both are compatible as long as information and its privacy are considered at each stage.

5.4. The IADM programme is ensuring that appropriate governance and process is in place for the Council to manage and handle information so that risks are treated and opportunities to share and use information are realised.

5.5. The Council has also established an Information Governance Group (IGG) which oversees the arrangements around Information Management in the Council.

5.6. Both IGG and IADM are central to leading and governing the Council's arrangements for managing information in compliance with relevant legislation including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).   This must be underpinned by strategy, policy, procedures, culture and behaviours.

5.7. The IADM programme has developed six core principles as part of the assurance framework; which are summarised below.

   5.7.1. *To provide clear leadership and guidance on how the organisation should manage, control and retain information.*

   The programme is focussed on instilling corporate standards, policies and business practices to provide the required leadership and governance.

   5.7.2. *Create, grow and foster a culture that values information.*

   The programme continues to work with data owners and the whole organisation through roadshows, workshops and projects to develop a

culture in the council which values the appropriate management of information and data. The change to the email retention policy is an example of how changes to how we view information can be challenging but achievable for the organisation.

5.7.3. Enable and assure compliance.

Understanding compliance is key to services achieving it, therefore it is a key objective of the programme to create an understanding of legislation and that information sharing is seen as an opportunity; when it is done with the correct controls and measures. The introduction of GDPR has reengaged focus on this and work is on-going to educate staff on the sharing and disclosure of information.

5.7.4. Create and embed corporate information standards and frameworks.

Information Management now forms part of the corporate annual assessment and the programme will continue to document and publish standard working frameworks for information practices across the authority. Information should be in a managed state at all times throughout its lifecycle, and where possible technology should be used to automate and control this. Implementation of key technologies such as Electronic Document and Records Management System (EDRMS), Enterprise Content Management (ECM) and protective marking / classifications are ensuring the council is standardising and protecting information.

5.7.5. Champion the accuracy, availability and integrity of information.

The Programme through a number of projects has increased the accuracy and integrity of address data. Prior to this, the Council's address data was classed as low quality, frequently falling below the national standard as governed by GeoPlace (the public sector partnership that oversees the national address gazetteer). Currently address data is within the highest levels of quality with the Council being awarded with gold standard for address data. Consequently, the availability of address data has also increased with more council services being able to use and trust the dataset, which has had a direct benefit on services such as Council Tax.

5.7.6. Use information to create intelligence.

Information across the authority must align to acceptable quality standards for it then to be used in meaningful and reliable ways to inform

decision making and service delivery. There is on-going work under IADM to establish data management and quality frameworks.

5.8. During 2018/19 the IADM programme delivered a number of focussed workshops with Heads of Service and roadshows and drop-ins for staff with the aim of clarifying the importance of information governance.

5.9. There are a number of projects being delivered to manage information across the various channels for the cleansing, deduplication and rationalisation of files, applications and records. This has the potential to allow the Council to safely remove information (upwards of half a million electronic files) no longer required by the Council which is either duplicated or past its retention date, this will ensure compliance with internal policy, and legislation and improve data quality and accessibility.

5.10. The Email Retention policy of two years has been approved and communicated; this will remove duplicate information held in the email system and support the requirements of GDPR. Information must reside with relevant case files or in central repositories (such as a case or content management solution) to ensure that it forms part of informed decision making, that it is accessible, secure and retained as per the retention assigned to the case.

5.11. A new e-learning training package (Protecting and Managing Information) has been developed and issued to officers to ensure consistent and compliant management of information across the authority. This training is mandatory for all officers to complete.

6. Implications of the Recommendations

6.1. Legal Implications

6.1.1. The Council must comply with GDPR, the Data Protection Act 2018, the Computer Misuse Act 1990, the Freedom of Information Act 2000 and other relevant legislation particularly those relating to retention of information.

6.1.2. GDPR has brought in substantially higher levels of penalties for data controllers than the previous legislation, up to €20 million and has introduced fines for data processors. The Council needs to understand what data they control and what is procesed on their behalf and build data protection into it's day to day processes to ensure that it and organisations processing data on its behalf are compliant.

6.2. **Finance Implications**

6.2.1. There are no financial implications but as the report highlights, failure to appropriately manage data and information could leave the council open to financial penalties.

6.3. **Policy Implications**

6.3.1. The Council's internal policies on Data Protection, ICT Security and Information Assurance will reflect any changes identified as part of the GDPR, the Data Protection Bill and the Data Protection Act 2018.

6.4. **Equality Implications**

6.4.1. Equality impact assessments will be considered when required.

6.5. **Human Resources Implications**

6.5.1. Under the new GDPR data subjects can obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. This requirement cannot be met if information is not managed in a compliant manner or used as a storage mechanism for information.

6.6. **Risk Management Implications**

6.6.1. Any changes to the risk profile of information and the Council will be detailed within the corporate risk register.

6.7. **Rural Communities Implications**

6.7.1. There are no direct implications for rural communities.

6.8. **Implications for Children & Young People/Cared for Children**

6.8.1. There are no direct implications for children and young people.

6.9. **Public Health Implications**

6.9.1. There are no direct implications for public health.

6.10. **Climate Change Implications**

6.10.1. There are no direct implications for climate change.

7. **Ward Members Affected**

7.1. Implications are borough wide

8. Consultation & Engagement

8.1. The Information Governance Update has been considered by the Audit and Governance Committee in July 2018.

9. Access to Information

9.1. There is no additional information.

10. Contact Information

10.1. Any questions relating to this report should be directed to the following officer:

Name: Gareth Pawlett
Job Title: Head of ICT Services and Chief Information Officer
Email: Gareth.Pawlett@cheshireeast.gov.uk