AUDIT, CRIME & DISORDER AND SCRUTINY COMMITTEE
26 NOVEMBER 2016

INFORMATION GOVERNANCE

Report of the:	Head of Legal & Democratic Services
Contact:	Simon Young
Urgent Decision?(yes/no)	No
If yes, reason urgent decision required:	
Annexes/Appendices (attached):	None
Other available papers (not attached):	

REPORT SUMMARY

A report to update members in relation to the Council's arrangements for Information Governance, in light of previous audit reports and good practice.

RECOMMENDATION (S)	*Notes*
(1) That members note the current position in respect of the Council's Information Governance arrangements and determine what future reporting they wish to receive on this subject.	

1 Implications for the Council's Key Priorities, Service Plans and Sustainable Community Strategy

1.1 Information Governance arrangements do not directly feature in the Council's key priorities and the applicable service plans. However, information governance is indirectly important to delivering against some of those key priorities. Poor information governance would have general implications for the Council's finances, for example if fines were imposed.

2 Background

2.1 "Information Governance" is a term which covers the standards, policies and procedures which govern the integrity, security and use of information within an organisation.

2.2 Information Governance covers a wide variety of areas of work. For example, the report on this agenda relating to Data Quality is part of the framework for assuring the integrity and use of certain information.

2.3 Information Governance covers all the information held by the Council and all the formats, devices and locations where that information is held.

2.4 As the topic is so broad, within the confines of a single report it is possible only to give a flavour of the work which is being undertaken.

2.5 The context as to why this subject is important, and what are our responsibilities is drawn from a number of sources, including:

2.5.1 Information rights and responsibilities

- *Data Protection Act 1998*
- *Freedom of Information Act 2000*
- *Environmental Information Regulations 2004*

2.5.2 Government Openness and Transparency Agenda

2.5.3 Council business priorities

2.5.4 Public Sector Network connection requirements

3 Where are we now? Where are we headed?

3.1 What do we want to achieve?

3.1.1 Efficient and appropriate use and sharing of data within the Council and with partners and customers

3.1.2 Security matched to risk

3.1.3 Restrictions on access according to role

3.1.4 Efficient Storage, Retrieval and Destruction systems

3.1.5 Organisation-wide appreciation of the issues

3.1.6 Detailed disaster recovery and business continuity

3.2 How are we doing this?

3.2.1 Governance Framework

- *Senior Information Risk Owner*
- *Information Asset Owners*
- *Individual staff and members*
- *Information Governance Group*

3.2.2 Good records management – which helps staff to manage the "Information Mountain"

3.3 Security breaches are a financial risk for Epsom and Ewell as well as for our public reputation. We can, and do, have technological security in place, but all staff and members hold the key to information security in their everyday work.

3.4 What protection do we have from threats?

3.4.1 Technology - Network, Virtual desktops, protection against threats.

3.4.2 Processes - Saving records securely, sending sensitive information securely, making sure records are accessible but protected.

3.4.3 Staff - Training, awareness, control.

3.5 The Information Governance Group has developed an action plan to address the key issues.

3.6 A number of internal audit assessments have been undertaken in recent years, and officers have sought to implement the recommendations in those reports. Most recently, a report on Information Governance was finalised on 23 October 2015. This gave reasonable assurance that the controls in place are suitably designed and consistently applied (Amber/Green). However, it also identified issues which require to be addressed. These comprised 1 medium- and 8 low- priorities for action, as set out in the agreed action plan in the report.

3.7 Some incidents do occur, but none has, so far, been "serious" according to the Information Commissioner's guidance. Breaches have been contained and, where appropriate, measures have been taken in an effort to prevent recurrence.

4 Financial and Manpower Implications

4.1 ***Chief Finance Officer's comments:*** The cost of ensuring adequate information governance arrangements is embedded within general overheads. Good information governance should be part of all services. The implications of not complying with statutory requirements could be significant. For example, the Information Commissioner has the power to issue monetary penalties up to £500,000 for breaches of the Data Protection Act 1998.

5 Legal Implications (including implications for matters relating to equality)

5.1 ***Monitoring Officer's comments:*** Information Governance concerns all of the Council's functions. There are several statutory duties engaged, of which the requirements of the Data Protection Act 1998 are key. The Act requires that the Council comply with the data protection principles, which relate to how personal information is acquired, kept, used and disposed of. For the purposes of this report, the most important principle is principle 7. This states that "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

5.2 Various actions across departments (particularly ICT) seek to meet the above requirement.

6 Sustainability Policy and Community Safety Implications

6.1 There are no implications arising directly from this report. Data protection requirements are engaged in relation to community safety work, and the arrangements are considered to be adequate.

7 Partnerships

7.1 It is important that appropriate arrangements are in place with all contractors and partners with whom we exchange data.

8 Risk Assessment

8.1 The risks in relation to information governance are organisational, technical, financial and reputational. Whilst it is impossible to eliminate all risk, the aim is to ensure that sufficient controls are in place to meet the objectives set out in paragraph 3.1. The level and nature of controls implemented must be balanced against the cost of those controls, both in cash terms and impact on productivity. Although the recent audit report is a snapshot of some issues, it is considered that the conclusion would also be a fair assessment of the Council's current overall level of assurance.

9 Conclusion and Recommendations

9.1 In conclusion, it is considered that the Council's arrangements for Information Governance are adequate, balancing our statutory obligations, the threats which exist, and the costs of control solutions. It is recommended that members note the report and determine whether and how they wish to be updated in future.

WARD(S) AFFECTED: N/A