Appendix 3 – Information Governance	
Reporting Officer:	John Walsh, Town Solicitor
Contact Officers:	Sarah Williams, Programme Manager

3.0	**Main report**
3.1	**Description of risk** The Information Governance risk, as captured in the Council's Corporate risk register is phrased as follows: '**Poor Information governance results in non-compliance with legislation and best practice standards.**'
3.2	**Risk Owner** Accountability for the management of this corporate risk has been assigned to John Walsh, Town Solicitor.
3.3	**Risk assessment** Following detailed review of the corporate risks, this risk was assessed in terms of 'impact' and 'likelihood' (using the Council's risk scoring system, see Appendix 1) as follows: Impact – 4 (major) Likelihood – 4 (likely) If the Council does not effectively manage personal data there is a risk of a financial penalty of up to £0.5m being levied by the Information Commissioner (which has the potential to increase to 4% of annual turnover if the UK follows the proposed EU approach from 2018). If the Council does not effectively manage information security, there is a risk of cyber attacks or intentional or unintentional data breaches. The impact of these would be 'major' from a financial and reputational perspective. The likelihood is currently assessed as 'likely' as while there has been progress in this area in relation to the delivery of awareness training for officers and Members and the development of policies and procedures in relation to Data Protection, further work is required to mitigate the risk. The target risk rating is: Impact – 4 Likelihood – 3 (possible)
3.4	**Current measures in place to manage the risk** The key controls that are in place to manage this risk are: ▪ Dedicated Information Governance Unit (formerly called Records Management

	Unit) in place ▪ Data Protection Policies and Procedures approved by Council in February 2016 ▪ Data Protection Training has been provided to 2300 staff, 100 decision-makers including the Corporate Management Team, with video and booklet versions provided to non-office staff ▪ There is a central logging system which is used to record and manage requests for information ▪ Following a high-profile data breach in 2012, an Information Governance Group was established with officers from Information Governance, Legal Services, AGRS and Digital Services, which is chaired by the Town Solicitor, and meets every two months. This group has developed, prioritised and is in the process of implementing a work plan of policies/procedures, reporting processes, staff training, communications and audit/compliance.
3.5	**Performance** The Information Governance Group (IGG) has developed a work plan to prioritise and develop policies and procedures for: A. **Information management** (how information is created, described, used, stored, archived and disposed of) B. **Information compliance** (the legal framework and standards to ensure that information management is within the law) C. **Information security** (the confidentiality, integrity and availability of information within the organisation and when sharing with partners) D. **Information assurance** (the practice of assuring and managing information risk) The IGG has in the last year: • developed and rolled out policies and procedures for data protection; • continued to provide data protection training to staff; • continued to communicate to staff particularly on the protection of data during the planned accommodation move; • developed a Freedom of Information (FoI) protocol to staff to ensure that Chief Officers are made aware of any relevant FoI requests The IGG is currently developing: • a corporate CCTV policy to ensure uniformity and compliance with the relevant laws and codes of practice; • an approach for planning for the impact of the new European General Data Protection Regulation whose approach may also be implemented in the UK by the Information Commissioner's Office; • an Information Security Policy
3.6	**Areas for improvement** The Group over the next year also plans to develop an updated Retention and Disposal Policy and Procedures; an updated Information/Records Management Policy; an approach to introducing Privacy Impact Assessments; and also a longer-term approach to corporate Information Assurance including the consideration of the implementation of

	an Electronic Document and Records Management System.