Risk Supporting Statement: CR16

Risk Owner: Chamberlain

Risk	Loss or mishandling of personal or commercial information could result in harm to individuals, a breach of legislation such as the Data Protection Act 1988 which incurs a monetary penalty of up to £500,000. Breaches can also incur compliance enforcement action, corruption of data and significant reputational damage. To ensure the protection of information at the City Corporation a number of controls and risk owners must be exerted which span IT infrastructure, information policy, physical handling, online access and sharing and everyday behaviour within and outside the City Corporation **Links to: All Strategic Aims and Key Policy Priorities.**	**Gross Risk**	**R**
		Likelihood	**Impact**
		5	3

Detail	There is a need to emphasise the importance of information governance as a discipline and the challenges it presents in the digital age (wider than the Data Protection Act) encompassing guidance and linkages to compliance, controls, behaviours, risks etc in relation to different types of information we handle and to sustain this engagement within organisation. Suggestions of how this can be achieved is provided in the accompanying report.

Issues

- Lack of Member and staff awareness of, and engagement with required behaviour with regards to information handling
- Office moves/relocations increase the possibility of losing or misplacing personal information.
- Transferring personal information to third parties, e.g. when contracting out services.
- Incorrect/accidental disclosure or loss of personal information, e.g. when sending personal information using any medium.
- Insufficient security in place to protect personal information across the City Corporation: only social care information is encrypte/protectively marked.
- lack of attention to risks posed by NOT sharing appropriate information - e.g. danger to life of vulnerable adults
- Increasing complexity and volume of information increasing costs

Controls

* Central monitoring & issuing of guidance and communications exists for data protection compliance (DP) (since 2003), along with nominated senior officer responsibility, Access to Information Network with departmental reps ***(Deputy Town Clerk)***
* DP awareness written into corporate employee policies as a requirement ***(Director of HR)***
* DP: Employee Data Protection Policy requirement to complete the corporate DPA e-learning course ***(Director of HR)***
* DP: Rolling program of tailored DPA training presentations for all staff and Members ***(Information Officer)***
* DP: Record of all presentation attendees and e-learning sign-offs kept for audit purposes ***(Information Officer)***
* DP: Awareness emails sent biannually to all staff ***(Information Officer)***
* DP: Other awareness raising tools used when highlighting key issues ***(Information Officer)***
* DP: Some monitoring of data processor contracts to ensure DPA compliance ***(Chief Officers of All Departments where Data Processors Operate)***
* IS recently appointed a Technical Solutions Officer to scrutinise and refresh existing policy around cybersecurity and technology infrastructure risk in partnership with Agilisys the IS strategic partner to the City.

Summary	**Net Risk**	A
* All Members and officers should be aware of 'good practice' in relation to handling information - but more needs to be done to address the opportunity and risk of information as business asset in CoL via policy refresh, staff and Member engagement, training and guidance. The accompanying report makes recommendations for next steps. * Personal information, in whatever format it is held, should be kept secure at all times. Appropriate polices, procedures and tools should be in place, regarding the management of personal information, including share, transfer, disclose, transport and destruction of information. * Compliance audits undertaken by Town Clerk's Information Officers are underway across the organisation to monitor DP adherence and suggest improvements. * The e-learning training course should be reviewed at regular intervals. At present the module covers DP however there is scope for this module to cover wider issues in relation to information security and management * In addition, the IS division will work in partnership with the Town Clerk's department in ensuring that relevant policies are refreshed at regular intervals, communicated and understood and to enforce necessary technological controls. * The risk owner for CR16 is the Chamberlain. However, every Department has a responsibility for the personal information it processes, and therefore all Chief Officers must assume responsibility to ensure compliance with Information Governance.	**Likelihood**	**Impact**
	3	3
	Control Evaluation	
	A	