CR08 - Information Governance and Data Compliance

Owner: Keane, Brian Position: Head of Governance

Impacts Upon	Reviewed	Next Major Review Date
▪ CP8 - Discharge of Statutory Obligations	31/12/2017	30/09/2018

Major Review Frequency

Quarterly

If	Then
If the Council does not adopt a holistic response to data and information governance	Then it may be unable to demonstrate statutory compliance

Background

The Council requires an Information Governance Framework to ensure information is dealt with efficiently, effectively and in compliance with statutory provisions and regulations. The General Data Protection Regulation (GDPR) applies in the UK from 25 May 2018, replacing the Data Protection Act 1998, imposin a much tougher data protection regulatory framework. Also on the horizon is Electronic Data Protection Regulation (EDPR).

Inherent Likelihood	Inherent Impact
Almost Certain (5)	Major (4)
Timescales dictated for FOIA and EIR request response. GDPR requirement to notify ICO of breaches within 72 hours. Changes to timescales for Subject Access Requests (SARs). It is necessary to be able to evidence compliance in all areas of GDPR. There are changes to the way consent is obtained and individuals rights over data held about them.	Breach and non-compliance carries risk of enforcement action and increased financial penalties from the Information Commissioners Office (ICO). Reputation would suffer.

Current Controls

Existing policies relating to FIA and EIR. GDPR project group set up and project plan underway. Corporate Information Asset Register established and being reviewed. Electronic database identification underway. Awareness campaign has begun with employees. Regular monitoring by Governance Group. Browne Jacobson have been employed as legal consultants and are looking at Corporate policies and reviewing Privacy Notices.

	Residual Risk	DoT	Foreseeable Ri
Risk Rating	21	▲ ➡	18
Risk Likelihood	Likely (4)	■ ➡	Moderate (3)
Risk Impact	Major (4)	■ ➡	Major (4)

Additional actions to mitigate risk (4Ts)

Appoint/Nominate Data Controller. Data retention policy to be reviewed/refreshed. Corporate policy/proce rollout and training across the Council. Fair Processing Notices require updating. Data sharing agreement to be reviewed, updated or drafted. Data Impact Assessments to be carried out as necessary.