

SDC HIGH LEVEL ACTION PLAN

AS AT 03.01.2018

Ref	Action	Target Date	Current Position/ Proposed Actions	Responsible Officer
1	<p>Policy Framework</p> <p>To review the Council's existing information governance policy framework (including data protection, freedom of information and records management) and to amend as necessary to reflect best practice and/or current legislation.</p> <p>Develop a Communications plan to refresh awareness of existing policies and to give regular reminders to staff on information governance issues.</p>	<p>Ongoing</p> <p>Ongoing</p>	<p>Revised policies adopted 2014.</p> <p>Policies are being reviewed in conjunction with NYCC and to reflect changes in legislation brought about by GDPR</p> <p>Periodic reminders given via information screen, posters and intranet updates</p>	

2	<p>Training</p> <p>To provide a series of training sessions for Members and officers on information governance matters, including the updated policy framework, the maintenance of information asset registers and the application of the council's data sharing agreements.</p>	30 April 2018	<p>Previously delivered</p> <p>Further all Member briefing to be held in May 2018 to coincide with introduction of GDPR</p>	Dem Services
	<p>Review information governance induction requirements include this and refresher training in the organisational development plan.</p>	completed	<p>Senior Managers Data Protection training held December 2017</p>	
	<p>Ensure employees complete mandatory training</p>	30 April 2018	<p>Previously completed in 2015 – Staff to undergo refresher training for GDPR</p> <p>Reports to be provided to Heads of Service of employees still to complete mandatory training</p>	
3	<p>Appoint Information Asset Owners (IAOs) for each key group of information assets</p>	30 April 2018	<p>Consider amendment of appointed Officers as IAOs following organisation review in preparation for GDPR</p>	GDPR Working Group
		30 April	<p>Support IAOs to update Information Asset Registers -</p>	

	Departments to review and maintain their information asset registers.	2018		
4	<p>Carry out annual risk awareness training for those with access to personal data</p> <ul style="list-style-type: none"> • Identify groups of staff and their training needs • Develop training packs for different groups • Deliver selected training • Monitor delivery of training • Carry out awareness campaign 		Further training to be rolled out as part of the organisation development strategy	Business Dev & Improvement
5	<p>Develop data sharing protocols with 3rd party suppliers & delivery partners</p> <ul style="list-style-type: none"> • Identify groups, exposure and needs • Prepare required data sharing agreements with partner organisations • Check decisions to share are recorded and that data sharing arrangements are in place • Develop appropriate awareness information packs • Ensure requirement is included in contracts 	Ongoing	SDC is signed up to the overarching Info Sharing Arrangements county wide	

	<ul style="list-style-type: none"> • Deliver training where appropriate 			
6	<p>Information Risk Policy</p> <p>Review policy further to NYCC taking on IT support</p> <p>Information risks will be considered by all services and significant risks identified through this process will be included in the service bases risk registers.</p>		To be considered as part of GDPR implementation	GDPR Working Group
7	<p>Develop Information Risk Register</p> <ul style="list-style-type: none"> • Register monitored regularly • Highest risks fed into corporate risk register • IAOs identified in Information Risk Registers 		To be reconsidered alongside work on corporate and service based risk registers	Heads of Service
8	<p>Information Security</p> <ul style="list-style-type: none"> • Develop Information Security Policy covering both IT and non IT based data • Communicate current system for IT Security to staff • Access to and use of sensitive data monitored • Member's ICT Acceptable Use policy 		<p>Agree monitoring process</p> <p>Ensure that Members IT provision is included as part of the IT Security Policy</p>	Business Dev & Improvement

	<ul style="list-style-type: none"> Managers to cascade messages to staff regarding the need to lock personal and confidential information away at the end of the day. Arrangements to address any issues with availability of storage, broken locks or absence of keys and places to store keys that may prevent information being locked away. Assigning responsibility for ensuring that shared archive rooms are locked at the end of the day and/or when not being used. Whether to schedule further information security checks on a regular basis. Checking on action taken to raise awareness of data security amongst staff and reporting of data breaches. 	<p>completed</p> <p>completed</p>	<p>completed</p> <p>key storage boxes to be fitted</p> <p>Final arrangements for securing archive rooms to be agreed</p> <p>Next sweep will take place between January and March 2018</p> <p>Noted increase in breach reporting indicating awareness</p>	<p>Assets</p> <p>Assets</p> <p>Veritau/Solicitor to Council</p>
9	<p>Privacy Notices</p> <p>To review the Council's existing privacy notices to reflect best practice and/or legislation.</p>	<p>30 April 2018</p>	<p>Action to review in relation to GDPR</p>	<p>GDPR Working Group</p>

	Prepare a privacy notice that applies to information collected across a range of Council functions and make available on the Council website			
10	<p>FOI</p> <p>Consider responsibility for the administration of requests to pass to the Customer Contact Centre and processes will be clearly defined and timescales agreed. This will include:</p> <p>Logging of requests immediately</p> <p>Differentiation of requests, FOI, EIR and SAR</p> <p>Process and agreed timescales for chasing requests and escalating them if they are delayed</p>		<p>Review completed – arrangements remain with Business Support. Significant improvement made.</p> <p>Will be reviewed again for GDPR compliance</p>	GDPR Working Group
11	<p>Corporate records retention and disposal schedule</p> <p>Prepare a consolidated corporate records retention and disposal</p>	30 April 2018	To be completed as part of GDPR preparations	GDPR Working Group

	<p>schedule in line with the document retention policy (this will apply to all records held and in all formats and will be made available throughout the organisation).</p> <p>Communicate to staff</p>			
--	---	--	--	--