GDPR ACTION PLAN

Governance Framework					
Workstream	**Objective**	**Actions**	**Officer**	**Status**	
• Review/revise policies and procedures	• The Council has checked its procedures to ensure that it can deliver the rights of individuals under the GDPR. • The Council has implemented appropriate technical and organisational measures to show it has considered and integrated data protection into its processing activities.	• Determine policies and procedures in scope and policy owners	OMT	Initial list of policies in scope before Friday 15 December	• Ensure policies cover all the rights individuals have, including how personal data would be deleted or provided electronically and in a commonly used format • Management support and direction for data protection compliance in a framework of policies and procedures. • Compliance with data protection policies with regular reviews of the effectiveness of data handling and processing activities and security controls.
		• Collate changes needed for each policy	JH	Before 19 January 2018	
		• Policy changes approved	OMT	Feb or March full Council, if necessary	
		• Publish revised policies		Feb or March 2018	
		• Ensure template letters/documents compliant with revised policies			
• Privacy Impact Assessments	• The Council understands when it must conduct a PIA and has processes in place to action this. • The Council has a PIA framework which links to its existing risk management and project management processes. • Good practice to adopt a privacy by design approach and to carry out a	• Design new process and form – to include reference to project management and risk management processes	JH	Draft PIA process and form before 29 December 2017	The GDPR includes provisions that promote accountability and governance. The Council should put into place comprehensive but proportionate governance measures including: • A privacy by design
		• Publication			
		• Training	SMT/OMT	Before implementation – April 2018	
		• Ongoing review and audit			

	privacy impact assessment as part of this. A privacy by design and data minimisation approach has always been an implicit requirement of the data protection principles. However, the GDPR will make this an express legal requirement. The Council should: ○ Review the ICO guidance on Privacy Impact Assessments (PIAs); ○ Implement a plan to introduce the new GDPR Data Privacy Impact Assessments within the Council; and ○ Implement procedures to link PIAs to other risk management and project management processes.				approach such as Privacy impact assessments; • Internal data protection policies; • Staff training; • Internal audits of processing activities; and • Reviews of internal HR policies.
• Data Protection Officer	• The Council has designated responsibility for data protection compliance to a suitable individual within the organisation (a Data Protection Officer).	• Scope requirements of DPO role	JH	8 December 2017	
		• Implement DPO role		31 January 2018	
		• Publicise – website, staff newsletter etc	Corporate Services	31 January 2018	
• Data Breaches	• The Council has implemented appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively. • The Council has mechanisms in place to assess and then report relevant breaches to the ICO where	• Determine current practices in relation to data breaches	JH	15 December 2017	GDPR will bring in a breach notification duty across the board. The Council should: • Implement appropriate procedures to ensure personal data breaches are detected, reported
		• Determine any gaps and produce actions for changes (to include reporting and notification procedure)	JH	29 December 2017	
		• Collate and apply changes to data breach procedure	JH	31 January 2018	

	the individual is likely to suffer some form of damage, e.g. through identity theft or confidentiality breach. • The Council has mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms.				and investigated effectively; and • Put mechanisms in place to assess and then report any breaches to the ICO where the individual is likely to suffer some form of damage, e.g. through identity theft or confidentiality breach.
Data Collection and Use					
• Data Audit	• Council has documented what personal data is held, where that data came from and who it is shared with. • The Council has planned to conduct an information audit across the organisation to map data flows.	• Establish what categories of information are held in each team	OMT	Initial list of categories of information held before Friday 15 December	Organise an information audit, across the organisation or within particular business areas; • Document what personal data is held, where it came from and who it is shared with; • Develop policies and procedures in order to ensure the accuracy of this document detailing the information held on an on-going basis; • The Council has planned to conduct an information audit across the organisation to map data flows.
		• Identify what personal data is included in each category, where it came from, and who it is shared with	OMT	Before Christmas	
		• Identify any data subject to 'higher risk processing'			
		• Particular issues to be included on risk register			
		• Periodic data audit at regular intervals in future		Ongoing	
		• Review retention and access schemes			
• Consent process	• The Council has reviewed how it seeks, records and manages consent. • The Council has reviewed the systems currently used to record consent and implemented appropriate mechanisms in order to ensure an effective audit trail. The GDPR is clear that businesses must	• Scope definition and requirements of consent			• As an organisation of fewer than 250 employees, the Council is required to maintain records of activities related to higher risk processing. • Aeas that could cause compliance problems under the GDPR and to
		• Determine methods for capturing and monitoring consent			
		• Options paper for review	SMT / OMT		
		• Implement options			

	be able to demonstrate that consent was given. The Council should: • Review consent mechanisms to make sure they meet the GDPR requirements on being specific, granular, clear, prominent, opt-in, documented and easily withdrawn; and • Review the systems currently used to record consent and implement appropriate mechanisms in order to ensure an effective audit trail.				be recorded on the Council's risk register.
• Privacy Notices	• The Council has reviewed its current privacy notices and has a plan in place to make any necessary changes in time for GDPR implementation. • The Council has reviewed the various types of processing it carries out. It has identified the lawful basis for its processing activities and documented this. • The Council has explained its lawful basis for processing personal data in its privacy notice(s). Many organisations will not have thought about their lawful basis for processing personal data. The Council should: • Conduct an information audit across the organisation to map data flows; • Document what personal data is held, where that data came from and who it is shared with; • Look at the various types of data processing carried out, identify the lawful basis for carrying it out and document it; and • Explain the lawful basis for processing personal data in Council privacy notice(s).	• Determine current practices and controls for maintaining privacy notices (printed and electronic, e.g. website) • Determine any gaps and produce actions for changes • Collate and apply chances to privacy notices			When the Council collects personal data it currently has to give people certain information, such as its identity and how it intends to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things the Council will have to tell people. The Council should: • Read the ICO's Privacy notices code of practice which reflects the new requirements of the GDPR; and then • Review the Council's current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

Third Party Management					
• List of Third Parties		• Collate list of all third parties within scope – i.e. parties with whom the Council contracts and shares personal data			
		• Establish central record or incorporate additional field in existing record to register relevant third parties			
• Standard Contract Terms		• Develop standard terms to incorporate both DPA and GDPR compliance	JH / SD	31 December 2017	
		• Incorporation of standard terms in all relevant contractual negotiations	AR / SD	31 December 2017	
		• Edit standard terms to GDPR only compliance	JH / SD	20 April 2018	
		• Incorporation of standard terms in all relevant contractual negotiations	AR / SD	1 May 2018	
• High Risk Third Parties		• Agree ongoing action plan to move existing contractual parties on to new contract terms	SD		
Retention and Disposal					
• Agreed and published retention periods for Personal Data		• Determine current retention periods and formatting			
		• Review period and highlight any gaps			
		• Where gaps exist highlight for legal review			
		• Options paper for best method of presenting			
		• retention periods to staff and public			
		• Implement options for retention, presentation and management			
• Establish and implement process for managing and monitoring retention periods		• Determine and collate all areas dependent on the retention schedule			
		• Document and agree process for maintaining schedule and communicate to affected staff			
• Agree and establish a process for the destruction of Personal Data		• Determine current controls and risks around electronic destruction of Personal Data			
		• Determine current controls and risks around physical destruction of Personal Data			

		• Implement agreed solution and establish monitoring controls			
Rights					
• Right to complaint		• Scope and document changes needed to complaints process			• The Council supports the data protection lead through provision of appropriate training and reporting mechanisms to senior management. • The Council has reviewed its procedures and has plans in place for how it will handle requests from individuals for access to their personal data within the new timescales outlined in the GDPR. • The Council has reviewed its procedures and has plans in place for how you will provide any additional information to requestors as required under the GDPR.
		• Agree implementation plan			
		• Deliver changes with training and awareness for appropriate staff			
• Right to correction, deletion and objection		• Scope and document GDPR requirements			
		• Benchmark requirements against current processes			
		• Agree changes and plan for implementation			
		• Implement changes with training support			
• Right to access		• Scope and document GDPR requirements			
		• Benchmark changes required against current processes			
		• Agree changes and plan implementation			
		• Implement changes with training support			
• Data portability		• Scope and document GDPR requirements			
		• Benchmark changes required against current processes			
		• Agree changes and plan implementation			
		• Implement changes with training support			
Security					
		• Scope and document incident response and notification process			
		• Benchmark requirements against current processes			

		• Agree changes for implementation	SMT		
		• Scope and document encryption requirements under GDPR			
		• Benchmark requirements against current processes			
		• Agree changes for implementation	SMT		
		• Scope and document confidentiality requirements under GDPR			
		• Benchmark requirements against current controls			
		• Agree changes for implementation	SMT		
		• Implement changes with training support			
		• Scope and document integrity requirements under GDPR			
		• Benchmark requirements against current controls			
		• Agree changes and plan for implementation	SMT		
		• Agree changes and plan for implementation	SMT		
Systems and Technology					
• Collated list of required system changes		• Collate systems in scope and changes needed from other workstreams			
		• Determine costs and resources needed for each change			
		• Document requirements for approval			
		• Agree action plan based on approval			
• Collated list of requirements for data portability		• Determine systems in scope for data portability requirements			
		• Determine costs and resources needed for each change			
		• Document requirements for approval			

		• Agree action plan based on approval			
• Deployment of anonymisation standards and processes		• Determine purposes where identification is not required			
		• Document anonymisation and pseudonymisation processes			
		• Scope and agree areas where can be applied			
		• Implement changes with training and support			
Training and Awareness					
• Scope and deliver training programmes for key roles	• Decision makers and key people in the Council are aware that the law is changing to the GDPR and appreciate the impact this is likely to have. • The Council is raising awareness across the organisation of the changes that are coming.	• Determine key roles and teams for dedicated training			• Check its current systems will support the rights of individuals under the new legislation, for example deleting electronically held personal data on request. The Council should: • Clearly set out its approach to the new GDPR legislation and assign responsibilities for managing the change; • Assess and identify areas that could cause compliance problems and record these on the Council's risk register
		• Determine training requirements for key roles			
		• Draft training programme			
		• Deliver training programme			
• Scope and deliver ongoing awareness programme	• Plan for a more general awareness campaign across the Council to educate staff on the changes to the current legislation and highlight how these changes will impact them. • The Council has developed and implemented a needs-based data protection training programme for all staff.	• Determine training needs for all staff based on changes in organisational redesign			
		• Draft training package for both face to face and e-learning			
		• Deliver training package			