

APPENDIX A - GDPR ACTION PLAN

Governance Framework				
Workstream	Objective	Actions	Status	
Review/revise policies and procedures	<ul style="list-style-type: none"> <li>The Council has checked its procedures to ensure that it can deliver the rights of individuals under the GDPR.</li> <li>The Council has implemented appropriate technical and organisational measures to show it has considered and integrated data protection into its processing activities.</li> </ul>	☐ Determine policies and procedures in scope and policy owners	Complete	<ul style="list-style-type: none"> <li>Ensure policies cover all the rights individuals have, including how personal data would be deleted or provided electronically and in a commonly used format</li> <li>Management support and direction for data protection compliance in a framework of policies and procedures.</li> <li>Compliance with data protection policies with regular reviews of the effectiveness of data handling and processing activities and security controls.</li> </ul>
		☐ Collate changes needed for each policy	With DPA Assist	
		☐ Policy changes approved	April 2018	
		☐ Publish revised policies	By end April 2018	
		☐ Ensure template letters/documents compliant with revised policies	By end of April 2018	
Privacy Impact Assessments	<ul style="list-style-type: none"> <li>The Council understands when it must conduct a PIA and has processes in place to action this.</li> <li>The Council has a PIA framework which links to its existing risk management and project management processes.</li> <li>Good practice to adopt a privacy by design approach and to carry out a 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.</li> <li>The Council should:                             <ul style="list-style-type: none"> <li>Review the ICO guidance on Privacy Impact Assessments (PIAs);</li> <li>Implement a plan to introduce the new GDPR Data Privacy Impact Assessments within the Council;</li> <li>Implement procedures to link PIAs to other risk management and project management processes.</li> </ul> </li> </ul>	☐ Design new process and form – to include reference to project management and risk management processes	Draft PIA process and form before 31 March 2018 – ICO guidance and templates	<p>The GDPR includes provisions that promote accountability and governance. The Council should put into place comprehensive but proportionate governance measures including:</p> <p>A privacy by design approach such as:</p> <ul style="list-style-type: none"> <li>Privacy impact assessments;</li> <li>Internal data protection policies;</li> <li>Staff training;</li> <li>Internal audits of processing activities; and</li> <li>Reviews of internal HR policies.</li> </ul>
		☐ Publication	30/04/2018	
		☐ Training	TBC	
		☐ Ongoing review and audit	Ongoing	
☐ 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	Complete	
		☐ Implement DPO role	Complete	
		☐ Publicise – website, staff newsletter etc	Ongoing	

<input type="checkbox"/> Data Breaches	<input type="checkbox"/> The Council has implemented appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively. <input type="checkbox"/> The Council has mechanisms in place to assess and then report relevant breaches to the ICO where the individual is likely to suffer some form of damage, e.g. through identity theft or confidentiality breach. <input type="checkbox"/> 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.	<input type="checkbox"/> Determine current practices in relation to data breaches	Policy and Procedure in place / being updated	GDPR will bring in a breach notification duty across the board. The Council should: <ul style="list-style-type: none"> <li><input type="checkbox"/> Implement appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively; and</li> <li><input type="checkbox"/> 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.</li> </ul>
		<input type="checkbox"/> Determine any gaps and produce actions for changes (to include reporting and notification procedure)	31/03/2018	
		<input type="checkbox"/> Collate and apply changes to data breach procedure	30/04/2018	

Data Collection and Use				
Data Audit	<ul style="list-style-type: none"> <li>• Council has documented what personal data is held, where that data came from and who it is shared with.</li> <li>• The Council has planned to conduct an information audit across the organisation to map data flows.</li> </ul>	<input type="checkbox"/> Establish what categories of information are held in each team	Information Asset Register circulated	Organise an information audit, across the organisation or within particular business areas; <ul style="list-style-type: none"> <li>• Document what personal data is held, where it came from and who it is shared with;</li> <li>• Develop policies and procedures in order to ensure the accuracy of this document detailing the information held on an on-going basis;</li> <li>• The Council has planned to conduct an information audit across the organisation to map data flows.</li> </ul>
		<input type="checkbox"/> Identify what personal data is included in each category, where it came from, and who it is shared with	By end of March	
		<input type="checkbox"/> Identify any data subject to 'higher risk processing'	5 <sup>th</sup> April 2018	
		<input type="checkbox"/> Particular issues to be included on risk register		
		<input type="checkbox"/> Periodic data audit at regular intervals in future	Ongoing	
		<input type="checkbox"/> Review retention and access schemes	May 2019	
Consent process	<ul style="list-style-type: none"> <li>• The Council has reviewed how it seeks, records and manages consent.</li> <li>• The Council has reviewed the systems currently used to record consent and implemented appropriate mechanisms in order to ensure an effective audit trail.</li> </ul> <p>The GDPR is clear that businesses must be able to demonstrate that consent was given. The Council should:</p>	<input type="checkbox"/> Scope definition and requirements of consent		<ul style="list-style-type: none"> <li>• As an organisation of fewer than 250 employees, the Council is required to maintain records of activities related to higher risk processing.</li> <li>• Areas that could cause compliance problems under the GDPR and to be recorded on the Council's risk register.</li> </ul>
		<input type="checkbox"/> Determine methods for capturing and monitoring consent		
		<input type="checkbox"/> Options paper for review		
		<input type="checkbox"/> Implement options		

	<ul style="list-style-type: none"> <li>Review consent mechanisms to make sure they meet the GDPR requirements on being specific, granular, clear, prominent, opt-in, documented and easily withdrawn;</li> <li>Review the systems currently used to record consent and implement appropriate mechanisms in order to ensure an effective audit trail.</li> </ul>			
Privacy Notices	<ul style="list-style-type: none"> <li>The Council has reviewed its current privacy notices and has a plan in place to make any necessary changes in time for GDPR implementation.</li> <li>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.</li> <li>The Council has explained its lawful basis for processing personal data in its privacy notice(s).</li> </ul> <p>Many organisations will not have thought about their lawful basis for processing personal data. The Council should:</p> <ul style="list-style-type: none"> <li>Conduct an information audit across the organisation to map data flows;</li> <li>Document what personal data is held, where that data came from and who it is shared with;</li> <li>Look at the various types of data processing carried out, identify the lawful basis for carrying it out and document it; and</li> <li>Explain the lawful basis for processing personal data in Council privacy notice(s).</li> </ul>	<input type="checkbox"/> Determine current practices and controls for maintaining privacy notices (printed and electronic, e.g. website)	April 2018	<p>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.</p> <p>The Council should:</p> <ul style="list-style-type: none"> <li>Read the ICO's Privacy notices code of practice which reflects the new requirements of the GDPR; and then</li> <li>Review the Council's current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.</li> </ul>
		<input type="checkbox"/> Determine any gaps and produce actions for changes		
		<input type="checkbox"/> Collate and apply changes to privacy notices		

Third Party Management				
<input type="checkbox"/> List of Third Parties		<input type="checkbox"/> Collate list of all third parties within scope – i.e. parties with whom the Council contracts and shares personal data	April 2018	
		<input type="checkbox"/> 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		
		☐ Incorporation of standard terms in all relevant contractual negotiations		
		☐ Edit standard terms to GDPR only compliance		
		☐ Incorporation of standard terms in all relevant contractual negotiations		
☐ High Risk Third Parties		☐ Agree ongoing action plan to move existing contractual parties on to new contract terms	May 2018	

### Retention and Disposal

☐ Agreed and published retention periods for Personal Data		☐ Determine current retention periods and formatting	From information asset register	
		☐ Review period and highlight any gaps	April 2018	
		☐ Where gaps exist highlight for legal review	April 2018	
		☐ Options paper for best method of presenting		
		☐ retention periods to staff and public	Early May 2018	
		☐ Implement options for retention, presentation and management	May 2018	
☐ 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		<p>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.</p>
		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				
		<input type="checkbox"/> Scope and document incident response and notification process		
		<input type="checkbox"/> Benchmark requirements against current processes		
		<input type="checkbox"/> Agree changes for implementation		
		<input type="checkbox"/> Scope and document encryption requirements under GDPR		
		<input type="checkbox"/> Benchmark requirements against current processes		
		<input type="checkbox"/> Agree changes for implementation		
		<input type="checkbox"/> Scope and document confidentiality requirements under GDPR		
		<input type="checkbox"/> Benchmark requirements against current controls		
		<input type="checkbox"/> Agree changes for implementation		
		<input type="checkbox"/> Implement changes with training support		
		<input type="checkbox"/> Scope and document integrity requirements under GDPR		
		<input type="checkbox"/> Benchmark requirements against current controls		
		<input type="checkbox"/> Agree changes and plan for implementation		
Systems and Technology				
<input type="checkbox"/> Collated list of required system changes		<input type="checkbox"/> Collate systems in scope and changes needed from other workstreams		
		<input type="checkbox"/> Determine costs and resources needed for each change		
		<input type="checkbox"/> Document requirements for approval		
		<input type="checkbox"/> Agree action plan based on approval		
<input type="checkbox"/> Collated list of requirements for data portability		<input type="checkbox"/> Determine systems in scope for data portability requirements		

		<input type="checkbox"/> Determine costs and resources needed for each change		
		<input type="checkbox"/> Document requirements for approval		
		<input type="checkbox"/> Agree action plan based on approval		
<input type="checkbox"/> Deployment of anonymisation standards and processes		<input type="checkbox"/> Determine purposes where identification is not required		
		<input type="checkbox"/> Document anonymisation and pseudonymisation processes		
		<input type="checkbox"/> Scope and agree areas where can be applied		
		<input type="checkbox"/> Implement changes with training and support		
<b>Training and Awareness</b>				
<input type="checkbox"/> Scope and deliver training programmes for key roles	<input type="checkbox"/> 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. <input type="checkbox"/> The Council is raising awareness across the organisation of the changes that are coming.	<input type="checkbox"/> Determine key roles and teams for dedicated training		<ul style="list-style-type: none"> <li>• Check its current systems will support the rights of individuals under the new legislation, for example deleting electronically held personal data on request.</li> </ul> <p>The Council should:</p> <ul style="list-style-type: none"> <li>• Clearly set out its approach to the new GDPR legislation and assign responsibilities for managing the change;</li> <li>• Assess and identify areas that could cause compliance problems and record these on the Council's risk register</li> </ul>
		<input type="checkbox"/> Determine training requirements for key roles		
		<input type="checkbox"/> Draft training programme		
		<input type="checkbox"/> Deliver training programme		
<input type="checkbox"/> Scope and deliver ongoing awareness programme	<input type="checkbox"/> 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.	<input type="checkbox"/> Determine training needs for all staff based on changes in organisational redesign		
		<input type="checkbox"/> Draft training package for both face to face and e-learning		
		<input type="checkbox"/> Deliver training package		