APPENDIX A - GDPR ACTION PLAN

-		_	
Gova	rnanco	Framev	vork
UUVE	inance	ITAILEV	VUIN

Workstream	Objective	Actions	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.	Determine policies and procedures in scope and policy owners	Complete	•
	 The Council has implemented appropriate technical and organisational measures to 	Collate changes needed for each policy	With DPA Assist	•
	show it has considered and integrated data protection into its processing activities.	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	 The Council understands when it must conduct a PIA and has processes in place to action this. The Council has a PIA framework 	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	The acc put gov
	which links to its existing risk management and project management processes.	Publication	30/04/2018	Ap
	 Good practice to adopt a privacy by design approach and to carry out a privacy impact 	2 Training	ТВС	•
	 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; Implement procedures to link PIAs to other risk management and project management processes. 	Ongoing review and audit	Ongoing	- •
Data Protection Officer	 The Council has designated responsibility for data protection compliance to a suitable individual within the organisation 	Scope requirements of DPO role	Complete	_
	(a Data Protection Officer).	Implement DPO role	Complete	_
		Publicise – website, staff newsletter etc	Ongoing	

- 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.

he GDPR includes provisions that promote ccountability and governance. The Council should ut into place comprehensive but proportionate overnance measures including:

privacy by design approach such as:

- Privacy impact assessments;
- Internal data protection policies;
- Staff training;
- Internal audits of processing activities; and Reviews of internal HR policies.

Data Breaches	The Council has implemented appropriate procedures to ensure personal data breaches are detected, reported and	?	Determine current practices in relation to data breaches	Policy and Procedure in place / being updated	GDP the b The 0	
	?	investigated effectively. The Council has mechanisms in place to assess and then report relevant breaches	?	Determine any gaps and produce actions for changes (to include reporting and notification procedure)	31/03/2018	a a
to the ICO where 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.	?	Collate and apply changes to data breach procedure	30/04/2018	r ii		
				e b		

Data Audit	 Council has documented what personal data is held, where that data came from and who it is shared with. 	 Establish what categories of information are held in each team 	Information Asset Register circulated	
	 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 	By end of March	
		Identify any data subject to 'higher risk processing'	5 th April 2018	
		Particular issues to be included on risk register		
		Periodic data audit at regular intervals in future	Ongoing	
		Review retention and access schemes	May 2019	
Consent process	The Council has reviewed how it seeks, records and manages consent.	 Scope definition and requirements of consent 		
	 The Council has reviewed the systems currently used to record consent and implemented appropriate mechanisms in 	 Determine methods for capturing and monitoring consent 		
order to ensure an effective audit trail. The GDPR is clear that businesses must be able to demonstrate that consent was given. The Council should:	Options paper for review			
	Implement options			

PR will bring in a breach notification duty across board.

e Council should:

- Implement appropriate procedures to ensure personal data breaches are detected, reported 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.

ganise an information audit, across the ganisation or within

rticular 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.

As an organisation of fewer than 250 employees, the Council is required to maintain records of activities related to higher risk processing.

Areas that could cause compliance problems under the GDPR and to be recorded on the Council's risk register.

F		•		
	 Review consent mechanisms to make sure they meet the GDPR requirements on being specific, granular, clear, prominent, opt-in, documented and easily withdrawn; Review the systems currently used to record consent and implement appropriate mechanisms in order to ensure an effective audit trail. 			
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 	April 2018	Whe has iden This the will The • 1

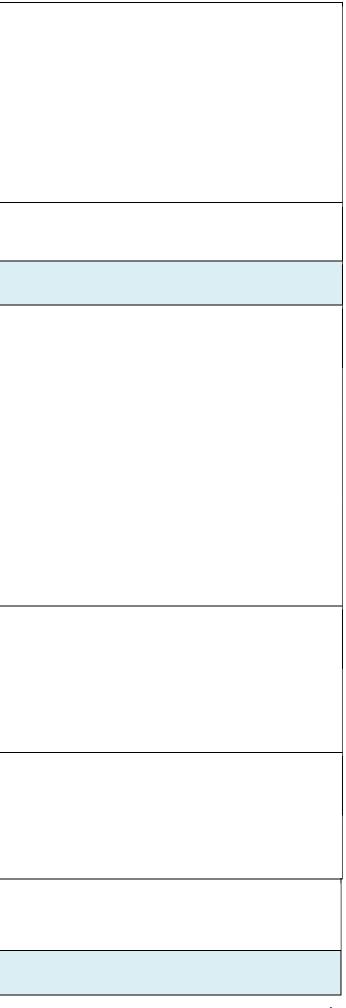
Third Party Management			
List of Third Parties	[2]	Collate list of all third parties within scope – i.e. parties with whom the Council contracts and shares personal data	April 2018
	2	Establish central record or incorporate additional field in existing record to register relevant third parties	

then the Council collects personal data it currently as to give people certain information, such as its entity and how it intends to use their information. his is usually done through a privacy notice. Under e GDPR there are some additional things the Council ill have to tell people.

e 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.

2 Standard Contract Terms	 Develop standard terms to incorporate both DPA and GDPR compliance
	 Incorporation of standard terms in all relevant contractual negotiations
	Image: Edit standard terms to GDPR only compliance
	 Incorporation of standard terms in all relevant contractual negotiations
I High Risk Third Parties	 Agree ongoing action plan to move existing contractual parties on to new contract terms
Retention and Disposal	
Agreed and published retention periods for Personal Data	 Determine current retention periods and formation asset formatting
	Image: Review period and highlight any gaps April 2018
	Image: Second state of the second s
	Options paper for best method of presenting
	retention periods to staff and public Early May 2018
	Implement options for retention, presentation and managementMay 2018
Establish and implement process for managing and monitoring retention periods	Determine and collate all areas dependent on the retention schedule
penous	Document and agree process for maintaining schedule and communicate to affected staff
Agree and establish a process for the destruction of Personal Data	Image: 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	



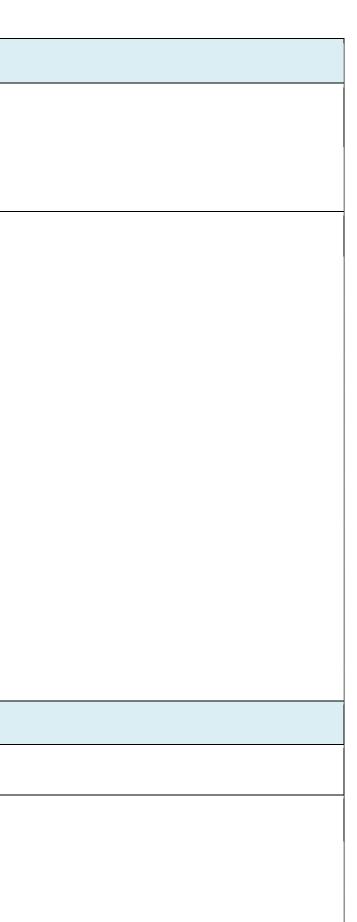
Right to complaint	2	Scope and document changes needed to complaints process	
	2	Agree implementation plan	
	[?	Deliver changes with training and awareness for appropriate staff	
Right to correction, deletion and objection	2		
	[?	Benchmark requirements against current processes	
	2	Agree changes and 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	
	2	Implement changes with training support	

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.

Scope and document incident response and notification process
 Benchmark requirements against current processes
Agree changes for implementation
Scope and document encryption requirements under GDPR
 Benchmark requirements against current processes
Agree changes for implementation
 Scope and document confidentiality requirements under GDPR
Benchmark requirements against current controls
Agree changes for implementation
Implement changes with training support
 Scope and document integrity requirements under GDPR
 Benchmark requirements against current controls
Agree changes and plan for implementation

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	
		Image: 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	1		
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	Determine key roles and teams for dedicated training	•
	appreciate the impact this is likely to have.	Determine training requirements for key roles	Th
	The Council is raising awareness across the organisation of the abareness that are coming	Image: Draft training programme	•
	changes that are coming.	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	 Determine training needs for all staff based on changes in organisational redesign 	
	current legislation and highlight how these changes will impact them. The Council has developed and	 Draft training package for both face to face and e-learning 	
	implemented a needs-based data protection training programme for all staff.	Deliver training package	

- 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