DRAFT GDPR IMPLEMENTATION PLAN FEBRUARY 2018

Ref	Title	Details	Responsible Officer	Time	Implementation
1	Data Protection Officer	The Council is required to appoint a Data Protection Officer or assign the role to a Senior Officer including agreeing the relationship with the Council's SIRO. • To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws. • To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. • To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).	Strategic Director Corporate Services	By 25 May 2018	Decision still required to be taken on this
2	Information Asset Registers, Privacy Notices, and Data Sharing Agreements	Asset registers need reviewing, approving by Information Governance Team and signing off by Assistant Directors to enable draft privacy notices to be completed Draft Privacy Notices to be prepared by the end of February 2018 Completed Privacy Notices to be prepared and Published for each Assistant Director area before 25 May 2018.	Head of Internal Audit, Insurance Information Governance and Risk	Before 25 May 2018	Asset registers need reviewing, approving by Information Governance Team and signing off by Assistant Directors to enable privacy notices to be completed Written Instructions and Pro forma on the preparation of Privacy Statements have been issued to all Assistant Directors. …..out of 32 have been

		Data Sharing Agreements need reviewing and central register kept			returned. Data Sharing Agreements need reviewing and central register kept
3	Data Protection Impact Assessments	The Council will need to ensure that privacy and data protection is a key consideration in the early stages of any projects/systems involving 'high risk' processing which include the following: • building new IT systems for storing or accessing personal data; • developing legislation, policy or strategies that have privacy implications; • embarking on a data sharing initiative; or using data for new purposes	System Owner/Project Manager is responsible for ensuring that a full Data Protection Impact Assessment is carried out on all IT systems and for all process changes that could impact on individuals' privacy	25 May 2018	Standard documents need putting on the Bradnet
4	ICT Compliance	WYPF will liaise with System Owner, ICT and the Information Governance Team • to implement any system changes to ensure GDPR compatibility • identify issues on right to erasure • identify issues on right to restrict processing • Rights in relation to automated decision making and profiling • Assess the impact on processes A risk assessment of each information asset should be undertaken before advising IT Services to undertake any further compliancy work to ensure any internal and external	Director of WYPF/System Owner	25 May 2018	

		resources are expended on the information assets posing the highest level of risk.			
5	Communication Strategy	Build on the initial communication on Bradnet with further communications on the GDPR. Communication set up for each month to all staff through Bradnet and Management comms announcing GDPR enactment	Head of Internal Audit, Insurance Information Governance and Risk	Before 25 May 2018	
6	Training Staff	Establish Training sessions and updated GDPR e-learning for Senior Management Training Key Staff Training General Training on GDPR for all staff Assessment of any Web Based Training to be delivered.	Head of Internal Audit, Insurance Information Governance and Risk	Before 25 May 2018	
7	Consents (including social media)	All Service Areas are required to review current consent issues to ensure they comply with the GDPR requirements	All Strategic Directors	Prior to 25 May 2018	
8	Update Policies and Procedures and GDPR Long Term Plan	Update Subject Access Policy and Procedure and Data Breach Procedure Determine a GDPR Policy to ensure the Council complies with the requirements	Strategic Director Corporate Services	Prior to 25 May 2018	The regular review of service areas' information asset registers - list of personal and non-personal information assets including IT systems held by departments

					Regular review of privacy notices Regular review of consents
9	Review Existing and Standard Contracts	Need to review the Council's **Procurement Contracts** with third party processors to ensure data protection clauses are GDPR compliant. Standard documents for new contracts also need updating to ensure GDPR compliant.	Strategic Director	Prior to 25 May 2018	Review Existing Contracts and Standard Documentation