Appendix 1

General Data Protection Regulation – Action Plan May 2017

What	ICO recommendation	Action	Proposed end date	By Whom	Progress
Raise awareness	• Ensure that that decision makers and key people in organisation are aware that the law is changing to the GDPR in 2018 • identify areas that could cause compliance problems under the GDPR	• Briefing to Members and Senior officers on GDPR and Action Plan • Briefing on GDPR and Action Plan to managers • Staff briefings • Project plan agreed and actions assigned to relevant officers	May 2017		
Data Protection Officers	• Designate a Data Protection Officer if required or someone to take responsibility for data protection compliance and assess where this role will sit within the organisation's structure and governance arrangements. • Assess whether current approach to data protection compliance will meet the GDPR requirements	• Appoint a Data Protection Officer • provide sufficient support to allow DPO to carry out role • ensure sufficient resources to carry out Controller responsibilities listed below	June 2017		

Conduct a personal information audit	• Document what personal data is held, where it came from and who it is shared with	• Carry out personal data audit
		  ○ Identify where special category personal data is being processed
		  ○ Identify where Minimisation and Accuracy of data collected is required
			September 2017		

		○ Identify where Consents are required ○ Identify where children's data retained ○ Identify where profiling is taking place ○ Identify processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (needs to comply with GDPR and a separate directive) • Compile and maintain a list of processing (Article 30) carried out by the authority (including by contractors and wholly owned companies) ○ Identify where personal data is being processed by a Data processor, ensure compliance with Article 40 (code of Conduct) or Article 42(Compliance certification) ○ Ensure processor holds a record of processing being carried out (Article 30) • Identify where privacy by design needs to be built into processing • Identify where personal data is not obtained from data subject.			

Consent	• Review and record how consent is sought and obtained (consent must be a positive indication of agreement, it cannot be inferred) • Review systems that are in place for recording consent – an audit trail is required	• Consent should not be relied upon unless absolutely necessary ICO has advised that public authorities should not need to rely on consent to carry out its functions	September 2017 (part of Data Audit)		
Children	• Review what systems are in place to verify individuals' ages and to gather parental or guardian consent for data processing activity for children (likely to be 13 or under but could be 16 or under – this is yet to be confirmed) • Review privacy notices relating to children – they must be in language that children understand	• Review how and why personal data or children is collect and used. • Where consent is relied upon ensure parental consent has been obtained for children under 13	September 2017 (part of Data Audit)		
International	• For organisations operating internationally, determine which data protection supervisory authority applies.	• Identify where personal data is stored and/or back up outside the EEA. • Gain an understanding of how Brexit will affect data storage on cloud based systems and whether the UK will have sufficient data protection standards to comply with EU standards or will special agreements be required.	Sept 2017 (part of Data Audit)		

Communicate privacy information	• Conduct a review of privacy notices and update where necessary (to include legal basis for processing, data retention periods, right to complain to ICO)	• Update privacy notices on all manual and electronic forms used to collect data • Update any consent including for direct marketing • Create a privacy dashboard on website for each dept. or processing carried out including data set out in GDPR	November 2017		
Legal basis for processing personal data	• Review the types of personal data processing that are carried out and identify and document legal basis for processing (e.g. consent)	• Undertake minimalisation of data collection • Implement privacy by design procedures • Review legal basis for data processing from data audit including the processing conditions set out in Article 6 and Article 9 (for special categories) of the GDPR • Review and update Data Retention and Destruction Polices • Create Information Asset Register	December 2017		
Individuals' rights	• Ensure procedures cover individuals' rights including: ➢ Subject Access ➢ to have inaccuracies corrected ➢ to have information erased (ensure that personal data can be deleted) ➢ to prevent direct marketing ➢ to prevent automated decision making ➢ to ensure data can be ported	Processes: • put in place a process to correct inaccuracies, rectification, erasure, restriction, automated decision making • put in place a process for preventing profiling • put in place a process for preventing direct marketing • put in place a process and facility for portability of data/self-service system	December 2107		

Subject Access Requests (SAR)	• Update subject access request procedures • Ensure that SARs can be handled within one month rather than 40 calendar days • Consider conducting a cost/benefit analysis of providing on-line access to personal information	Review and update data protection policy Review and update data subject access request procedure	January 2018		
Data breaches	• Review procedures for detecting, reporting and investigating personal data breaches • Determine which incidents would fall within the notification requirement if there was a breach • Develop policies and procedures for managing data breaches	• Update Security incident breach policies and procedures including a process for notification to ICO and to data subject where a breach is identified within the timescales set out in the GDPR	January 2018		

Data Protection by Design / Data Protection Privacy Impact Assessments	• Digest ICO guidance on Privacy Impact Assessments and determine when and how to implement PIAs within the organisation
	• Develop processes for including data protection controls at the design stage of new project involving the processing of personal data
		• Develop a process for carrying out Privacy Impact Assessment
		• Embed process into
		  ○ procurement process
		  ○ services reviews
		  ○ reports for committee/council
		  ○ project management
			January 2018		

Data Protection Training for all staff	• Set a timetable for relevant staff training for all staff	• Agree levels of training required for posts/depts. • Agree a training programme • Implement training programme • Agree a rolling programme to ensure compliance with GDPR	January 2018		
Compliance certification	• If required obtain a data protection certification to demonstrate compliance	• keep up to date on information and requirements coming out of the ICO or Article 29 working Party to ensure compliance with GDPR any code of conduct, code of practice or certification requirements	April 2018		