Appendix B General Data Protection Regulation (GDPR) Action Plan

V 0.4 December 2017

Ref	Action	Agreed action	Work completed to date	Target Date	Next Review	Progress Review Notes	Actions outstanding and resources required	Responsible Officer
	Issues under ICO's 12 Steps to take now					**At Dec 17**		
	1. Awareness							
	Training	Ongoing Data Protection training (Article 32 GDPR-testing effectiveness of organisational measures for security of processing) and ensure renewed every 2 years and non completion followed up. Include member training. Implement ongoing training needs plan.	All teams, IAO's and members training completed. Developed in house interactive e-learning package now up to 70% completion rate for all staff and rising. Need to continue to implement and monitor training needs plan.	Completed but ongoing	Dec-17	List of staff not having completed the e-learning went to AD Group in Dec 17. % includes staff on long term leave, maternity etc so % would be higher. Need to issue basic training sign off sheet for staff with limited or no access to personal data or PC	Need to target staff to complete e-learning on 2 year anniversary. Automate through software netconsent. Need to amend e-learning to remove references to DPA and add more detail on GDPR changes.	IGO/LDSM/BDITM
	Comms	Re-brand Data Protection (Article 32) Comms to use 'customer privacy' 'data privacy '. Re brand GDPR as Let's Get Data Privacy Ready. Raise awareness with GDPR Comms Plan.	Ongoing data protectors forum updates and Comms articles referring to GDPR. Have been posting now for over 1 year and records of these on Council's intranet city people. Have revised GDPR Comms plan moving towards 25 May 2018 (date GDPR in force)- 6 month plan.	Comms to be issued every month running up to 25/05/2018	Dec-17	Agreed 6 month plan with Comms and IG team	Monthly assistance from Comms. IG team to amend and approve.	IGO/COMMS
	Policies and Guidance	Draft GPDR Handbook for IAO's. Draft a GDPR policy to be implemented and agreed before May 2018 to replace Data Protection Policy and Summary sheet. Obtain approval and issue to staff.	All information management polices were reviewed and approved in May 2016. All polices available on City People. IAO's should actively monitor compliance with the Policies in their business areas. All policies are due for review and implementation by May 2018. GDPR Handbook drafted for IAO, issued to IAO's discussed in training and available on City People.	GDPR policy and summary sheet be issued to staff before May 2018	Dec-17	Need to draft high level policy for GDPR. Perhaps Data Privacy and Access to Information policy. Summary sheet to be issued to staff. Include data subject's enhanced rights and changes to SAR's	GDPR Policy to be drafted and agreed by IG team for committee approval and other policies reviewed.	IAO's IGO/LDSM/BDITM
	Regular item at team meetings	Consider incorporating data privacy as a regular agenda item at team meetings. Agree level for Data Protection issues to be discussed e.g. DMT/SMTs	Several IAO's are already incorporating need to ensure in all teams.	Quarterly	Jan-17	To be included in IAO's checklist to be issued Jan 18	IGO and LDSM have finalised for roll out in Jan 18	IAO's
	2. Information the council holds							
	Information asset audit	IMPs system to be fully populated and reports into Performance DMT	Information asset audit completed by IGO with all IAO's. IMPS system now fully populated with summaries and IAO's contacted to follow up and implement asset audit recs. IAO's previously given summary reports with own recs to implement	Audit completed recs to be followed up	Dec-17	All IAO's sent IMPs recs as reminder to summaries. Deadline to resond Nov 17. Need to follow up IAO's who have not responded.	IGO currently populating IMPS and following up recs with IAO's.	IGO
	Information asset register	Information assets registers should be updated, reviewed and risk assessed on a periodic basis by IAO's	Registers issued to all IAO's. Training provided to update as and when required and at least every 6 months. Needs to form part of IAO self assessment checklist. Any changes to registers need to provided to the IGO to update corporate register. Guidance in IAO GDPR Handbook.	Reviewed by IAO's every 6 months and as and when required.	Dec-17	To be included in IAO's checklist to be issued Jan 18	IGO and LDSM have finalised for roll out in Jan 18	IAO's
	Retention and disposal schedules	Ensure future adherence to retention and disposal schedules. This includes emails. Retention schedules updated and available on council's intranet.	R & D schedules updated and available on city people. IAO's responsibility to ensure compliance in their service areas. Needs to form part of IAO self assessment. Guidance in IAO GDPR Handbook.	Implementation reviewed by IAO's every 6 months and as and when required	Dec-17	To be included in IAO's checklist to be issued Jan 18	IGO and LDSM have finalised for roll out in Jan 18	IAO's
	Information sharing- with our data processors	Contracts with Processors Article 28 identify contracts for review and ensure these and new contracts are GDPR proof. Joined up approach with Legal and Procurement	Received terms and conditions from procurement Lincolnshire and need to review. IAO's to assist to identify in their areas contracts which may need to be reviewed or put into place. Guidance in IAO GDPR Handbook.	May-18	Dec-17			IGO/LDSM/PO and IAO's
	Information sharing- with other data controllers who are not processing on our behalf	Information Sharing Agreements should be reviewed and consolidated and a database held in Legal Services. All data shared with external bodies should be subject to an ISA	A database of existing ISA's has been created. Review dates to be plugged into Netconsent and consider amending them. IAO's to have responsibility to identify in their area where ISA's may be required and seek advice from IGO/LDSM to implement. Guidance in IAO GDPR Handbook.	May-18	Dec-17			IGO/LDSM and IAO's

Ref	Action	Agreed action	Work completed to date	Target Date	Next Review	Progress Review Notes	Actions outstanding and resources required	Responsible Officer
	ICO notification	Implement the DP fee notification process once decided http://www.actnow.org.uk/content/218. Monitor fees decision	Aware and monitoring decisions made	May-18	Dec-17			LDSM
	3. Communicating privacy information							
	Privacy statements	Information provided where personal data is collected- Article 13 GDPR. IAO's must identify and review Privacy Notices in their areas which require amendment to comply. Amendments to be made with assistance from IGO where required. Review Council's general privacy statement on website.	Responsibility for Privacy Notices in service areas allocated to IAO's training provided and guidance in IAO Handbook. IAO's to seek advice from IGO where required. IAO's have revised their Privacy statements in several areas. The Council's general statement has been reviewed by IAO's and is to be amended following approval.	May-18	Dec-17	To be included in IAO's checklist to be issued Jan 18	IGO and LDSM have finalised for roll out in Jan 18	IAO's IGO - LDSM
	4. Individual's rights	Rectification, right to be forgotten, data portability- Articles 16-20. Document the review and weeding process for software systems storing personal data. This task should have an assigned owner and be monitored. Develop plan for 'weeding' of data as part of R&D work.	Few systems have procedures for removal of personal data currently. The BDIT Manager has liaised with IAO's and contacted all suppliers of core systems. The responses received are varied and need to be assessed and plan actioned.	May-18	Dec-17	Suppliers have been in contact regarding GDPR changes to systems. I Trent for HR staff. Uniform for Planning. Civica for APP. Civica for Universal Housing.	Ongoing BDIT	BDITM/IAO's
	5. Subject access requests	Rights of access by the data subject- Article 15. Ensure we can comply with the additional rights of data subjects created by GDPR including the right to have their personal data deleted. Draft GDPR policy to replace the Data Protection Policy to include access to information request changes effective from May 18.	Policy to be prepared and reviewed following clarification of derogations in Data Protection Bill, and Comms plan to include access by subjects to data	May-18	Dec-17	Comms plan includes changes to access to information requests. GDPR and access to infromation policy to be drafted and summary sheet to be issued to staff by May 2018.	GDPR Policy to be drafted and agreed by IG team for committee approval.	LDSM/IGO
	6. Legal basis for processing personal da	Record of Processing Activities (ROPA)- Article 30 to be prepared based on the asset register to include data sharing details and legal basis for processing. ROPA database to be designed and implemented	Information regarding data held and information flows have been collated in the information asset register. Investigations are being undertaken as to how to build on these records and display them. the intention is to produce a basic record of processing activities by May with a view to expanding on this in due course, to be a full scale database or extending the asset register to provide more detail	May-18	Dec-17		Database to be developed or/and information to be added to asset register and/or ROPA statement	BDITM/IGO
	7. Consent	Ensuring whether we have valid Consent (Articles 7-8) from customer's where required by reviewing how we seek, obtain and record consent and whether we need to make any changes to comply with GDPR.	IAO's to assist IG team to identify areas where we are relying on consent alone to process personal data and review with assistance if necessary whether this consent is valid. Changes have already been made to consent statements in some areas. Guidance issued to IAO's In Handbook and face to face training.	May-18	Dec-17	To be included in IAO's checklist to be issued Jan 18	IGO and LDSM have finalised for roll out in Jan 18	IAO's
	8. Children	Identify any areas where we be may obtaining personal details and relying on consent from children under 16 years due to changes. DP Bill has reduced this to 13 years.	IAO's to assist IG team to identify areas where relevant and ensuring we have systems in place to verify individuals age and to gather partental or guardain consent for the data processing activity.	May-18	Dec-17	To be included in IAO's checklist to be issued Jan 18	IGO and LDSM have finalised for roll out in Jan 18	IAO's
	9. Data breaches	Ensure DP Breach Management (Articles 33-34) policy up to date and internal breach reporting system compliant with GDPR timescales for reporting. Monitor through IG group and officers for lessons learnt and trends.	Development of internal e-form Breaches being reported to IG Group. Internal breach reporting system effective with GDPR time scales i.e. 72 hours to report to ICO.	May-18	Dec-17	Comms Plan includes changes to breach reporting and time limts.	Data Protection Breach Management Policy to be amended to include GDPR changes and new time limits.	IGO/LDSM/BDITM
	10. Data protection by design and data protection impact assessments (DPIA's)							

Ref	Action	Agreed action	Work completed to date	Target Date	Next Review	Progress Review Notes	Actions outstanding and resources required	Responsible Officer
	Data protection impact assessments	Data protection Privacy Impact Assessments- Article 35 of GDPR Introduces a formal Policy to require a DPIA. Conduct a DPIA for new systems that involve the processing of personal data, or significant changes to existing systems. Such DPIA's should be signed off at an appropriate level and implemented into project planning at the earliest stage.	DPIA Guidance has been drafted along with templates and Comms. Needs to be implemented for new processes with maybe an e-form to assist - focus on those mandatory ones. Project management guidance to be amended Build DPIA into SPIT process (or replacement process) for new systems and training rolled out where required	May-18	Dec-17	Pilot DPIA's have been completed for the Rogue Landlord Project and identified that the process needed to be condensed as over complicated. Guidance and templates to be simplified and reissued. Further version trialled with BDIT and Audit Manager.	IGO has drafted further version after 2nd pilot and to be rolled out soon.	LDSM/BDITM/IGO Project Managers
	Build DPIA's into project planning	Review of Lincoln Project Model and Project Management	LDSM to meet with Policy to discuss once governance arrangements for projects are agreed	May-18	Dec-17			LDSM
	Security of processes	Security of Processing- Article 32 implement technical and organisational measures to ensure a level of security appropriate to the risk. Consider pseudonymisation capabilities where encryption not available. Ability to restore access to data in event of an incident and regular testing of effectiveness of measures.	ICT policies already in place including security and restoration of data following an incident. Need to raise awareness of risks and explore if pseudonymisation software is necessary. Internal Audit underway regarding security of applications.	May-18	Dec-17		Ongoing BDIT	BDITM
	Access to applications	Access requests for new starters should be made by appointed staff members with the appropriate authority. Network access should be suspended when staff are absent from work for an extended period, for example; due to maternity leave. Any failure by HR to notify IT of staff leavers or long-term absence should be treated as a security incident and reported to the IGO. Access to systems and drives should be reviewed regularly and at least every 6 months.	ICT policies already in place covering access requests and removal. In addition to this regular access reviews now being carried out in areas processing sensitive data such as Benefits every 6 months. Applications audit currently being undertaken by Audit. Previous Asset Audit identfied issues with Access in some systems and relevant recs to be followed up. Access reviews included in handbook issued to IAO's	May-18	Dec-17		Relevant System's team BDIT and IAO's	IAO's/AuditM/BDITM
	Testing of security measures	Testing effectiveness of security measures- Article 32. Prepare a Checklist for IAO's to complete following training in January 17 to ensure . Devise annual self assessment checklist for IAO's. Internal audit of IG	Handbook issued as guidance to checklist. Checklist to be issued annually. Include an aspect of information management in the 2017-19 Audit Plan where it is identified as a key risk by the ICO. The council could include records management as a standard item on the internal audit plan to ensure regular DPA compliance checks are completed. Sample monitoring of customer service calls including customer identification and verification questions already taking place.	Audit planned March 2018. Checklist issued to IAO's annually	Dec-17	An internal Audit for GDPR compliance is being programmed for Feb/March - AuditM to confirm	Internal Audit	IAO Audit
	Physical security and clear desk policy	IAO's to be reminded to carry out periodic spot checks of business areas adherence to the clear desk policy including the locking away of sensitive personal data and use of confidential waste bins. Also minimising the amount of personal data taken offsite.	Included in handbook. Transporting data securely between locations is included in REMOVAL guidance on city people. This was issued to staff on 31/08/16 via Data Protectors Forum and directly to Managers in key areas to provide to relevant staff.	Ongoing/Adhoc	Jan-18	To be included in IAO's checklist to be issued Jan 18	IGO and LDSM have finalised for roll out in Jan 18	IAO's
	11. Data protection officer's (DPO's)	Designating a data protection officer- Article 37-39 and assess where this role will sit within our organisation's structure and governance arrangements. Prepare report for CMT approval and appoint to role before May 18. Determine position in governance structure and ensure DPO has appropriate expertise.	Appointment of role considered at CMT on 17/10/17 and approved. JD drafted and to go to panel in Dec 17.	May-18	Dec-17		DPO to be appointed.	LDSM
	12. International	Determine which data protection supervisory authority the council comes under	The council will be under the UK supervisory body which will be the Information Commissioner's Office (ICO)	May-18				