General Data Protection Regulation (GDPR) Action Plan

V 0.6	Key									
	Outstanding- failure attracts higher level fines- 20 million Euros									
	Completed									
	Outstanding-failure attracts lower level fine -10 million Euros		At Dec 17	At Jan 18	At Mar 18					
Ref	**Action**	**Agreed action**	**Work completed to date**	**Work completed to date**	**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									
	1. Awareness									
1.1 Y	**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.	Completion rate to be reviewed again at the end of Jan 18 and issued to AD's after recent issuing of low risk dp training sheet for staff with no or very little contact with personal data.	Completion rate to be reviewed again at the middle of March 18 and issued to AD's . GDPR specific training via video/e learning/Netconsent to go to IAO/s SM's early from May	Completed but ongoing	Apr-18	List of staff not having completed the e-learning went to AD Group in Feb 18. The % includes staff on long term leave, maternity etc so % would be higher. Issued 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. Deliver GDPR specific training	IGO/LDSM/BD ITM
1.2 G	**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 article issued late Dec17-clear up on emails retained. Jan 18 article regarding all emails being potentially disclosable on Dp forum. GDPR visual introduction to be issued by comms end of Jan 18.	Jan 18 article regarding all emails being potentially disclosable on Dp forum. GDPR visual introduction issued by comms in Feb. Article on mandatory data breach reporting issued in March	Comms to be issued every month running up to 25/05/2018	Apr-18	Agreed 6 month plan with Comms and IG team	Plan complete -Monthly assistance from Comms. IG team to amend and approve comms before issuing.	IGO/COMMS
1.3 Y	**Policies, Guidance and procedures**	Draft GPDR Handbook for IAO's. Draft GDPR policies 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.	Ongoing	GDPR handbook circulated and checklist in draft has been issued. To be finalised with netconsent soon. GDPR policy drafted to PSC on 20 March 2018 and Exec on 26 March 2018	GDPR policy and summary sheet be issued to staff before May 2018 via netconsent	Apr-18	Handbook prepared and checklist being rolled out 24 January. Summary sheet to be drafted and issued to staff. Include data subject's enhanced rights and changes to SAR's.	GDPR Policy to be issued. Summary sheet to be drafted and issued to staff. Procedures on website for Subject Access Requests to be changed before May 18. All IM policies to be reviewed.	IAO's IGO/LDSM/BD ITM
1.4 G	**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.	Included in report to AD's Jan 18.	Has been recommended to all IAOs through training/checklist and then to AD's. SMTF have agreed to put it on their agenda.	Quarterly-ongoing for teams	Apr-18	Included in IAO's checklist issued Jan 18 and SM's reminded in Feb meeting	Completed	IAO's
	2. Information the council holds									

Ref	Action	Agreed action	Work completed to date	Work completed to date	Work completed to date	Target Date	Next Review	Progress Review Notes	Actions outstanding and resources required	Responsible Officer
2.1	**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	Outstanding recs being monitored in performance DMT. IAO's be chased again regarding outstanding recs.	Outstanding recs being monitored in performance DMT. IAO's be chased again regarding outstanding recs.	Audit completed recs to be followed up	Apr-18	All IAO's sent IMPs recs as reminder to summaries. Need to follow up IAO's who have not responded.	IGO following up recs with IAO's.	IGO
2.2	I**nformation asset register/ records of processing (ROPA)**	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.	Work being completed towards ROPA. Consolidating asset register and identifying legal basis for processing.	Work being completed towards ROPA. Consolidating asset register and identifying legal basis for processing. Included in IAO's checklist	Reviewed by IAO's every 6 months and as and when required.	Apr-18	Legal basis for processing being added and links to retention schedules and Sharing Agreements	IGO and BDIT resolved to have the ROPA developed before May 18	IAO/BDIT/IGO
2.3	**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. Form part of IAO checklist. Guidance in IAO GDPR Handbook.	Complete.	Complete.	Implementation reviewed by IAO's every 6 months and as and when required	Apr-18	Responsibility with IAO's	Complete save for monitoring	IAO's
2.4	I**nformation sharing-with our data processors-(Contracts)**	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.	CCS issued standard terms and conditions for contracts involving processing of personal data in Jan 18. Plan to list contracts and contact parties to agree variations where required.	Plan in place to list contracts and contact parties to agree variations where required. IAO's requested to populate contracts register and complete declaration in Mar 18. AD's to declare. Next stage to identify personal data contracts and prioritise. Obtain contact details to vary contracts	May-18	Apr-18	Progress with contracts and partnership register being up to date and sign off by IAOs and then AD's by 23 march then, we'll be able to contact suppliers	ID contracts where personal data and non framework to then contact suppliers	IGO/LDSM/PO and IAO's
2.5 G	**Information sharing-with other data controllers who are not processing on our behalf (ISA's)**	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. 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.	New ISA's being implemented and being identified for issue from new DPIA process.	New ISA's being implemented and being identified for issue from new DPIA process.	May-18	Apr-18	Complete and ongoing	Review dates in IAO checklists. Consider whether review dates can be monitored through Netconsent	IGO/LDSM and IAO's
2.6 G	**ICO fees**	£2900 for the organisation £40 for councillors	Pay in Aug. when registration is up	Ongoing	Ongoing	Aug-18	Apr-18	Complete and ongoing on annual basis	complete in Aug.	LDSM
3	**3. Communicating privacy information**									

Ref	Action	Agreed action	Work completed to date	Work completed to date	Work completed to date	Target Date	Next Review	Progress Review Notes	Actions outstanding and resources required	Responsible Officer
3.1 Y	**Privacy statements (also a Right to be informed)**	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.	Being amended as IAO's identify and approach IGO team for assistance.	Being amended as IAO's identify and approach IGO team for assistance.	May-18	Apr-18	Now included in IAO's checklist but ongoing	support and ongoing monitoring. Draft genarl priavacy notice for website. 'Your Personal Data'	IAO's IGO - LDSM
4	**4. Individual's rights**									
4.1 Y	**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.	Ongoing discussions with a number of suppliers APP, I Trent, Index making changes due to GDPR and offering products	Ongoing discussions with a number of suppliers APP, I Trent, Indox making changes due to GDPR and offering products.Oucome some products are offering free upgrades, some are offering enhancements for fee. Enhancements can be achieved currently althoguh would save time and resources. Need to assess cost/benefit and demand	May-18	Mar-18	Suppliers have been in contact regarding GDPR changes to systems. Uniform for Planning. Civica for APP. Civica for Universal Housing. Considering reports to teams re data being over x years old.	Ongoing BDIT	BDITM/IAO's
5	**5. Subject access requests (SAR)**									
5.1 Y	**Rights 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	Ongoing	GDPR Policy drafted and to go to PS March 18	May-18	Apr-18	Comms plan includes changes to access to information requests. GDPR policy drafted and summary sheet to be issued to staff by May 2018.	Summary sheet for public and staff to be developed, and issued, website to be changed.	LDSM/IGO
6	**6. Legal basis for processing personal data**									
6.1 Y	**Legal bases**	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	Being identified on asset register for ROPA.	Being identified on asset register for ROPA.	May-18	Apr-18	Ongoing	Database being developed or/and information to be added to asset register and/or ROPA statement	BDITM/IGO
7	**7. Consent**									

Ref	Action	Agreed action	Work completed to date	Work completed to date	Work completed to date	Target Date	Next Review	Progress Review Notes	Actions outstanding and resources required	Responsible Officer
7.1 Y	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.	Consents being altered as IAO's identify and approach IG team if required for assistance.	Consents being altered as IAO's identify and approach IG team if required for assistance.	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	**8. Children**									
8.1 G	**Obtaining personal data directly from 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 parental or guardian consent for the data processing activity.	Not identified applicable in any areas to date.	Not identified applicable in any areas to date.	May-18	Apr-18	Included in IAO's checklist	Complete - ongoing monitoring	IAO's
9	**9. Data breaches**									
9.1 G	**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.	Ongoing Policy and reporting process in place.	Ongoing Policy and reporting process in place.	May-18	Apr-18	Comms Plan includes changes to breach reporting and time limits.	Data Protection Breach Management Policy to be slightly amended to include GDPR changes and new time limits.	IGO/LDSM/BD ITM
10	**10. Data protection by design and data protection impact assessments (DPIA's)**									
10.1 G	**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	New simplified process developed and issued to IAO's across directorates for projects for completion. IGO assisting when requested.	New simplified process developed and issued to IAO's across directorates for projects for completion. IGO assisting when requested.	May-18	Apr-18	Rolled out guidance, training done, in IAO handbook and checklist. Ongoing	Complete-ongoing and monitoring.	LDSM/BDITM/ IGO Project Managers
10.2	**Build privacy by design (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	Ongoing discussions	Ongoing discussions	May-18	Apr-18	LPMM to be changed	Review of project model and incorporate DPIA process	LDSM

Ref	Action	Agreed action	Work completed to date	Work completed to date	Work completed to date	Target Date	Next Review	Progress Review Notes	Actions outstanding and resources required	Responsible Officer
10.3	**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.	Ongoing	Ongoing	May-18	Apr-18	Audit is ongoing	Ongoing BDIT	BDITM
10.4	**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 identified issues with Access in some systems and relevant recs to be followed up. Access reviews included in handbook issued to IAO's	Ongoing	Ongoing	May-18	Apr-18	Checklist includes this	Relevant System's team BDIT and IAO's	IAO's/AuditM/ BDITM
10.5	**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.	Ongoing	Ongoing	Audit planned 18/19. Checklist issued to IAO's annually	Apr-18	Ongoing	Internal Audit	IAO Audit
10.6 G	**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.	Continues to be implemented	Continues to be implemented	Ongoing/Adhoc	Apr-18	Checklist includes this	Complete-ongoing with monitoring	IAO's

Ref	Action	Agreed action	Work completed to date	Work completed to date	Work completed to date	Target Date	Next Review	Progress Review Notes	Actions outstanding and resources required	Responsible Officer
11	**11. Data protection officer's (DPO's)**									
11.1	**Data Protection officer**	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.	Job evaluation panel considering Jan 18.	Job approved, to be recruited March-18	May-18	Apr-18	Recruiting March 18	DPO to be appointed	LDSM
12	**12. International**									
12.1 G	**International supervisiory authotiy (ICO)**	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)	Ongoing	Ongoing	May-18	Complete	Included in the checklist and privacy statements	Complete and monitoring	IGO/LDSM
12.2	**International transfers**	Identify any areas where personal data is being transferred to a third country (outside EU and EEA) and if taking place ensure necessary safeguards are in place.	No areas identified although IT due diligence questions being drafted to include products to hosted in the UK although IT already applying in Polices	No areas identified although IT due diligence questions being drafted to include products to hosted in the UK although IT already applying in IT Policies	No areas identified although IT due diligence questions being drafted to include products to hosted in the UK although IT already applying in IT policies	May-18	Apr-18		To finalise due diligence IT questions to be raised when procuring products	BDITM