Information Governance and General Data Protection Regulation (GDPR) ongoing Action Plan 2018/2020

Appendix B

Infringement attracts higher level fine 20,000.00 EUR.

Infringement attracts lower level fine 10,000.00 EUR

Ref	Action	Agreed action	At June 18	At Sept 2018	At Dec 2018	Target Date	Next Review	Actions outstanding and resources required	Responsible Officer
	Issues under ICO's 12 Steps to take now								
	1. Awareness								
1.1 RED	**Training**	Ongoing Data Protection training (Article 5 GDPR- security, Article 32-testing effectiveness of measures for security) and ensure renewed annually or at least every 2 years with non completion being followed up. Include member training. Implement ongoing training needs plan.	As at the 19 June 18 90.5% overall completion – 64 not completed 91.9% higher risk – 50 not completed 77.8% low risk – 14 not completed	Stats 90.05% as at June 18 and rising. Teams, IAO's and new members trained. Purchased data protection videos for use.	Member training delivered 11th October 2018 follow up session for non-attendees being offered. AD's agreed to ongoing DP training being updated delivered by Dojo videos and questions to all staff through net-consent.	Ongoing-training to be renewed every 2 years for staff.	Jan-19	Need update on current figures and decide how to monitor delivery of renewal every 2 years. BDITM to provide up date on stats. Training vids	DPO/LDSM/BDITM
1.2 AMBER	**Comms**	Re-brand Data Protection (Article 32) Comms to use 'customer privacy' 'data privacy '. Re brand GDPR as Let's Get Data Privacy Ready. Re brand message GDPR Carrys On. Continue to raise awareness with GDPR and DP Comms Plan.	Comms continues to be issued as and when required.	ICO have issued bespoke Comms package for organisations 'Your data matters' to be utilised on ICO website. Also Dojo data protection vids now available. DPO informed service managers at forum in Sept 18. New Comms Plan drafted. New poster this month- for customers on screen downstairs. Poster for staff on stairwells	Comms issued image on customer facing computer screens and article in Our Lincoln magazine with link to your data privacy customer privacy notice in accordance with ongoing Comms Plan.	Ongoing plan forms part of Vision 2020.	Jan-19	Ongoing Comms plan for Oct 18-March 19 drafted by Comms needs implementing and monitoring.	COMMS/DPO
1.3 RED	**Policies, Guidance and procedures**	GDPR Article 5-security and Article 32-testing. GPDR Handbook for IAO's and annual Checklists. GDPR/DP policy implemented and Information management polices to be updated	Reviewed and amended IM Policies due to go to Audit 19/07/18 and Exec 21/07/18 for approval. Will be reissued with Comms to staff and uploaded into netconsent.	IM policies updated for GDPR and approved by Committee.	Updated IM polices have been uploaded into net-consent to be delivered with acknowledgement that staff are aware have been updated and are in net-consent. Separate acknowledgement of GDPR Policy already obtained.	Jan-19	Jan-19	Comms to go out. Staff to acknowledge receipt through netconsent - aware updated and where available not individual sign up to each policy.	IAO's /DPO
1.4 GREEN	**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		Checklists issued to IAO's July 18 to be returned by 28 Sept 18. Responses will then need to be reviewed and any follow up actions taken.	Checklists returned by IAO's Sep 18. Follow up meetings with non-completers and attendance at DMT's/SMT's where requested.	Ongoing	Jan-19	Assess response to checklists and follow up actions	IAO's/DPO
	2. Information the council holds								
2.1 AMBER	**Information asset audit**	IMPs system to be fully populated and reports into Performance DMT	Long term audit recs such as retention implementation in systems being chased through managers' AD's and CLT.	Need to clear up audit recs as majority dealt with or moved into applications review as system actions. All areas need to focus on long term actions relating to deleting and destroying data beyond retention.	Need to clear up audit recs as majority dealt with or moved into applications review as system actions. All areas need to focus on long term actions relating to deleting and destroying data beyond retention.	Audit completed long term actions ongoing	Jan-19	Delete or follow up outstanding actions on IMPS link with Applications Audit.	DPO/LDSM/BDITM
2.2 AMBER	**Information asset register/ records of processing (ROPA)**	Article 30 Records of processing Information assets registers should be updated, reviewed and risk assessed on a periodic basis by IAO's	Need to build on existing asset register. Will be issuing IAO checklist in July 18 and annually thereafter including maintaining asset register and assessing risks to assets.	See June 18	IAO's have confirmed assessment of assets and updating of their asset regsiter in checklists.	Reviewed by IAO's every 6 months and as and when required.	Jan-19	Need to build on existing records to improve and consider use of software now provided by LGA	IAO/BDIT/DPO
2.3 RED	**Retention and disposal schedules**	Ensure future adherence to retention and disposal schedules. This includes emails and systems. Retention schedules updated and available on council's intranet.		Provided to staff and customers via website.		Implementation reviewed by IAO's every 6 months and as and when required		Complete save for monitoring	IAO's/DPO

Ref	Action	Agreed action				Target Date	Next Review	Actions outstanding and resources required	Responsible Officer
2.4 AMBER	**Information 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	AD's chasing small number of IAO's yet to complete. AD's signed off process and DPO and Legal have started to amend on risk basis and processors who have contacted us.	Ongoing.LDSM and DPO dealing with Suppliers who have contacted CLC. Only handful of IAO's not completed contracts register. Need to progress	Ongoing.LDSM and DPO dealing with Suppliers who have contacted CLC. Only handful of IAO's not completed contracts register. Need to progress	Mar-19	Jan-19	ID contracts where personal data, prioritise according to sensitivity and non framework to then contact suppliers	DPO/LDSM/PO and IAO's
2.5 AMBER	**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		Need to ensure list comprehensive. Issue to staff. Upload on netconsent. ISA amnesty.	ISA template has updated for GDPR and is in use.	Completed but needs improving May 2019	Jan-19	Review dates in IAO checklists. Consider whether review dates can be monitored through Netconsent. Conintue to identify processs requiring a ISA and ISA that need updating	DPO/LDSM and IAO's
3	**3. Communicating privacy information**								
3.1 RED	**Privacy notices (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 DPO where required. Review Council's general privacy notice on website.		Council privacy notice to customers on website. The majority of service areas have produced service specific privacy notices	Council privacy notice to customers on website. The majority of service areas have produced service specific privacy notices	Ongoing/Adhoc	Jan-19	IAO's need to identify new processes requiring privacy notices and existing. This is covered in DPIA process too.	IAO's DPO
4	**4. Individual's rights**								
4.1 RED	**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.	Ongoing discussions with system providers.	Systems are capable of enforcing data subjects new rights. Although in some only manually. Will need to monitor whether automated add ons are required depending on volume of requests.		Ongoing	Jan-19	Ongoing BDIT. All areas need to prioritise deleting and destroying data beyond retention including in systems.	BDITM/IAO's/ DPO
5	**5. Subject access requests (SAR)**								
5.1 RED	**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.		New personal data requests process implemented prior to May 18 and working well	Requests are being complied with rountinely under the GDPR processes	Ongoing	Jan-19	Completed but ongoing.	DPO/LDSM
6	**6. Legal basis for processing personal data**								
6.1 AMBER	**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	Detailed in privacy notices and in asset register	As at June 18	As at Sept 18.	Ongoing	Jan-19	Database/ software to be considered or/and information to be added to asset register.	BDITM/DPO
7	**7. Consent**								
7.1 RED	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.				Ongoing/Adhoc	Jan-19	IAO's review through checklist.	IAO's/DPO
8	**8. Children**								
8.1 RED	**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. DPA has reduced this to 13 years. Article 8				Completed but ongoing		Complete - ongoing monitoring	IAO's/DPO
9	**9. Data breaches**								

Ref	Action	Agreed action				Target Date	Next Review	Actions outstanding and resources required	Responsible Officer
9.1 AMBER	**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.			Data breach policy and internal reporting system in place. Stats reported to CMT through IG Group quarterly	Completed but ongoing			DPO/LDSM/BDITM
10	**10. Data protection by design and data protection impact assessments (DPIA's)**								
10.1 AMBER	**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.		Improvements being made to guidance and templates in consultations with users. To be reissued to staff and made available on city people.		Ongoing/Adhoc	Jan-19	Ongoing resources needed from DPO to assist with DPIA's	LDSM/BDITM/DPO Project Managers
10.2 AMBER	**Build privacy by design (DPIA's) into project planning**	Review of Lincoln Project Model and Project Management		Improvements need to be made to imbedding in LPMM as staff have noted could be clearer need to complete DPIA.		Completed but ongoing	Jan-19	DPO to roll out amended DPIA process and LPMM to be amended to make need to complete clearer.	DPO/Policy
10.3 RED	**Security of processes**	Security of Processing- Article 32 and Article 5-security. 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.		Included in current review of applications with relavnt follow upactions being sent to IAO's and IT		Ongoing/Adhoc	Jan-19	Ongoing BDIT	BDITM
10.4 RED	**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.		Included in current review of applications with relevant follow up actions being sent to IAO's and IT		Ongoing/Adhoc	Jan-19	Relevant System's team BDIT and IAO's	IAO's/AuditM/ BDITM/DPO
10.5 AMBER	**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				Audit planned 18/19. Checklist issued to IAO's annually	Jan-19	Internal Audit. BDIT	IAO/BDITM AuditM
10.6 AMBER	**Physical security and clear desk policy**	Testing of security-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				Ongoing/Adhoc		Complete-ongoing with monitoring	IAO's
11	**11. Data protection officer's (DPO's)**								
11.1 AMBER	**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.				Completed but ongoing		Complete	DPO
12	**12. International**								

Ref	Action	Agreed action				Target Date	Next Review	Actions outstanding and resources required	Responsible Officer
12.1 RED	**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.				Completed but ongoing	Jan-19	Consideration to due diligence IT questions to be raised when procuring products	BDITM