Information Governance Action plan

July 2017

Appendix A

NOTE = Blue IN RIGHT HAND COLUMN ARE ONGOING MATTERS WHICH NEED TO BE MONITORED

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
Governance						
G.1	An information governance strategy should be developed and adopted that clearly sets out strategic and operational responsibility for data protection compliance.	There is no current strategy, although there is amount of work that has already been completed. This includes a raft of policies (some now aging) and some audit work, which again would probably be best to be reviewed. Current summary guides already in place are: • Data Protection • Freedom of Information • Record retention and Disposal • Information Management There is guidance on: • Data Protection • Freedom of Information • Information Management Roles and responsibilities • Knowledge Management	IG Strategy		LDSM/BDITM/IGO	Green
			Review and consolidate all existing policies.	Spring 2016	LDSM/BDITM/IGO	Green
			Seek approval from Officers and Members IG Strategy	 Executive approval obtained for the IG Strategy on 30/11/15	 LDSM/BDITM	Green

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
		• Records Management • Record Retention and Disposal And the following policies are also in place: • Data Protection • Freedom of Information • Information Management • Knowledge Management • Physical security • Records Management • Retention and Disposal Schedule Further guidance will be issued on: • The Government Security Classification Policy • Telephony Usage	Summaries to be prepared	End June 2016	LDSM	
G.2	The council should identify a Senior Information Risk Officer (SIRO) or equivalent, to provide dedicated oversight for information governance and risk issues, and to provide the Chief Executive with assurance. The SIRO's responsibilities should be incorporated into job descriptions and deliverables.	Thus far, this role has been partially accommodated through work by the Legal and Democratic Services Manager and the Business Development and IT Manager. However, it is not considered they have enough capacity to fulfil the tactical and operational roles which they are currently fulfilling in terms of Information Governance, nor do they have the status to meet the ICO's requirements i.e. likely a Board Member is required to be SIRO.	Formalise SIRO role and duties in Policies.	Early 2016, after the corporate restructure	LDSM/BDITM/IGO	Green
G.3	SIRO to monitor the progress of the Information Governance Action Plan	To be considered upon appointment.	Continued Reporting to AD and Audit, prepared by SIRO		LDSM	Blue

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
G.4	The council should nominate a specific committee or other body to provide a venue for oversight of information governance.	Business Needs Group have previously undertaken this role, it is felt that the Audit Committee are more appropriate.	It is suggested that this role could be performed by the Audit committee	Agreed Audit Committee 08/12/15	LDSM/BDITM	Green
G.5	The council should implement and manage a regular review cycle for all Information Governance policies so that they remain up to date and incorporate any necessary developments and changes in the law.	Reviews are currently done adhoc, due to the limited resource available. Internal audit periodically review parts of the Information Governance process. Whilst IT Security has a 'Substantial Assurance' rating currently, Information Governance is a red risk on the Annual Governance Statement.	Review policies annually or more frequently if required	Ongoing	LDSM/BDITM/IGO	Blue
G.6	The council should ensure that all revised and updated policies are made available to staff and that user declarations are introduced.	Policies are made available to staff through the Intranet. At log on to the IT network, staff are advised that they need to be aware of the policies. Some specific policies e.g. GCSx require staff with specific accesses to sign to say they will comply.	Publish policies when completed First policies complete Netconsent software purchased and to be implemented. Staff will be made aware of any new polices at log in and required to sign up to polices. This can then be evidenced.	Netconsent to be implemented from Autumn 2017	LDSM/BDITM	Amber
G.7	The Annual Governance	AGS is reported in the Strategic Risk register.	Continue to report	Ongoing	LDSM/BDIT	Green

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
	Statement findings to continue to be reported into the Strategic Risk Register				M	
G.8	Introduce a formal Policy to require Privacy Impact Assessments. Conduct a PIA for new systems that involve the processing of personal data, or significant changes to existing systems. Such PIA should be signed off at an appropriate level. Refer to the ICO Privacy Impact Assessment Handbook for further guidance.	No PIAs have been completed to date.	Develop PIA process. PIA Guidance has been drafted along with templates and Comms. Need to be implemented for new processes. Project management guidance to be amended	June 2017	LDSM/BDITM/IGO	Amber
			Build PIA into SPIT process for new systems	SPIT review pending. Ongoing	Project Managers	Red
Training & Awareness						
T.1	The Information Governance strategy should include responsibility at Member level for data protection training.	There is currently no Member with specific named responsibility for Data Protection	Identify Member for responsibility for IM.	Councillor Speakman appointed 08/12/15	LDSM/BDITM	Green
T.2	The council should consider appointing an Information Governance Officer.	Information Governance is currently shared between the Legal and Democratic Services Manager and the Business Development and IT Manager. There is considered a paucity of capacity to fulfil the role effectively currently.	Appointed September 2015	Done	LDSM/BDITM	Green

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
T.3	Develop a needs based training plan for data protection that sets out what data protection training staff will receive and at what frequency. It should address the generic training for all staff and those staff in specialist roles and be refreshed on an annual basis	Training is currently provided in an adhoc manner, and is considered inadequate to meet requirements currently. New staff receive an overview as part of the induction process, but there has been no actively planned IM training to managers for several years and almost none to front line staff other than the R&B shared service.	Develop plan as part of workforce development Staff teams have all received data protection briefings from the IGO. E-learning package is in place and has been rolled out to staff and two-yearly refresh, to be monitored through netconsent, once implemented Approval required for mandating training from CMT – AD's have confirmed that they will take responsibility for records management	Ongoing	LDSM/BDITM/IGO	Amber
T.4	Select a practical deadline for all council staff and members handling personal data as part of their job role to complete the mandatory data protection e-learning package. Completion should be monitored and evidenced by business area.	No e-Learning package is currently in place. Many staff have had no training except for some information passed down through Managers several years ago.	Develop or procure e-learning package- done As per T3	Ongoing	LDSM/BDITM/IGO	Green
			Ensure all staff trained and monitored As per T3	Ongoing	LDSM/BDITM/IGO	Amber

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
T.5	Once the new training plan and e-learning programme have been introduced, the IGO (or nominated individual) should monitor and report training metrics to the SIRO, relevant senior management team meeting and Audit Committee that has oversight of data protection compliance to provide a key performance indicator for DPA training completion rates.	There is no training programme in place.	Monitor training adequacy Report back results from netconsent and e-learning package	Ongoing	LDSM/BDITM/IGO	Blue
T.6	As part of the data protection training plan, the council should ensure that there are processes in place to identify any gaps in completion of the required training and that follow up procedures are adhered to and effective	There is no training programme in place.	Monitor Training Adequacy. Completion of the Data Protection Awareness Training is recorded against the staff members training records in I Trent system and reports can be produced identifying staff who have not completed this training.	Ongoing	LDSM/BDITM/IGO	Blue

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
T.7	Mandate DPA training as a part of the council's induction programme, with a particular focus on information security, data quality and the 8 Principles.	Some basic training is carried out at induction Is included in induction checklist	Link formal training to induction/e-learning training		LDSM/BDITM/HR	Green
T.8	Ensure that biennial refresher training is planned into the overall DP Training Programme	There is no training programme in place.	Build in biennial refresher training to all service plans	Ongoing	LDSM/BDITM/HR	Blue
T.9	The council should mandate DPA training for elected members, with further and more particular training for the portfolio-holding member.	Members received training on Information Governance in June 2016 and the slides shared with those not in attendance. It is not possible to make this compulsory but it will be rolled out every year and will be compulsory for new members. Members are given information relating to their responsibilities.	Develop and deliver training for Members and lead member in particular	July 2016	LDSM/BDITM/IGO/LDSM	Blue
T.10	The council should broaden the range of training material available to staff on the intranet and use awareness-raising materials to reinforce staff awareness such as the ICO 'Th!nk Privacy' material available on the ICO website.	A 'Data Protectors' forum is available on the Intranet and articles of interest are posted occasionally. There are currently 45 members. In addition, other information is made available on the intranet or through briefings occasionally	Develop more content and use regular briefings on Intranet	Ongoing	LDSM/BDITM/IGO	Blue

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
T.11	Consider incorporating data protection as a regular agenda item at team meetings.	Not held as a formal standing item, although some groups do discuss issues as they arise. The LDSM and BDITM occasionally attend DMTs with items of importance.	Agree level for Data Protection issues to be discussed e.g. DMT/SMTs	March 2016 onwards	LDSM/BDITM	Blue
Records Management						
R.1	Select a member of staff to formally oversee records management at the council. The post holder should work closely with Team Leaders to establish and implement a records management framework. (See c10 for associated recommendation)	The current IGO is undertaking work on this in conjunction with the SIRO.	IGO/SIRO	Ongoing	LDSM/BDITM/IGO	Green
R.2	Once appointed, the SIRO should register with the National Archives, subscribe to the monthly SIRO newsletter and consider completion of HMG Cabinet Office Protecting Information Training levels 2 and 3. Please see '*Local Public Service Data Handling* Guidelines*, version 2, August 2012*'.	Not completed	Subscribe SIRO to resources. The SIRO has attempted to access these although the courses are currently not available.		LDSM/BDITM	Amber
R.3	The council should formally appoint IGO	Completed	Appointed IGO		LDSM/BDITM	Green

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
R.4	Designate a policy owner for the Records Management Policy. Ensure that the Policy is periodically reviewed and amended to reflect change. Update the Records Management Policy and other relevant policies and procedures to reflect the current management structure and the allocation of records management responsibilities.	There is no current formal owner of the Records Management Policy	SIRO to be policy owner		Executive approval of Policy	Green
R.5	When the Records Management Policy has been updated, issue the Strategy to council staff and keep a record that it has been read and understood. Team Leaders should actively monitor compliance with the Strategy in their business areas.	Awaiting Records Management Strategy	Manage policies through log on processes/monitoring of training etc.		LDSM/BDITM/IGO/Managers	Blue
R.6	Adopt the Government Security Classifications Policy or equivalent in all business areas. Monitor the schemes	Guidance on GCSP will be reviewed, and needs to be covered more fully in training. Detailed implementation needs to be considered as part of the rollout of IM.	• Consider detailed implementation and implications. • Develop plan for further rollout	AD Group to consider in June 2017	LDSM/BDITM	Amber

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
	implementation and use.					
R.7	Incorporate records management into the corporate induction programme delivered to new starters. The data quality principles that relate to the adequacy, relevancy, accuracy and retention of personal data should be covered.	Corporate induction programme contains an awareness training on IM, although will need amending when a revised Corporate RM policy is agreed.	Reviewed and concluded that training covers the principles and IAO's will lead on records management side		HR/ LDSM/ BDITM	Green
R.8	The council could utilise readily available online training resources to supplement the proposed e-learning package. All staff with records management responsibilities should complete level 1 HMG Cabinet Office Protecting Information e-learning module or equivalent as part of their mandatory training. Please see '*Local Public Service Data Handling* Guidelines*, version 2, August 2012*'.	No e-Learning package is currently available however an alternative or equivalent to the level 1 package is in place. To be fully rolled out and mandate that people complete it	Consider use of these resources and how they will complement training plan Covered by National Archives and IGO training for IAOs		LDSM/BDITM/IGO	Amber
R.9	Include data protection and records	Some awareness message are included in the Data Protectors Intranet Forum, and messages are	Comms plan prepared and reviewed regularly	October 2015 – initially	LDSM/BDITM	Blue

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
	management awareness messages periodically in Weekly Briefs from the comms team and a comms plan	occasionally included in 'In Brief' corporate briefing.		completed and ongoing		
R.10	Allocate responsibility for approving new Privacy Notices to the IGO or IAO. The ICO would suggest using the ICO's Privacy Notices Code of Practice for guidance on the content and consistency of new notices.	No formal responsibility has yet been allocated.	Allocate responsibility for Privacy Notices Provide training for IAOs for developing Privacy Notices	September 17	IGO - LDSM	Red
R.11	Implement an overarching corporate retention schedule for physical and electronic records based on statutory retention requirements and relevant guidelines and allocate accountability for the schedules to IAO / Team Leaders. The council's retention schedules should be made available to all staff via the intranet.		Develop R&D schedule	Retention schedules have been provided to all IAO's. The corporate schedule needs to be made available to all staff on the intranet. November 2016	LDSM/BDITM/IGO	Green
R.12	It is recommended that		Review all old files first	September	LDSM/BDIT	Amber

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
	the council implement an archive project plan. In the short term records that no longer need to be retained should be identified and securely destroyed by each business area. In the long term the project plan should include implementation of a documented process in all business areas for the submission, storage, retention, recall and secure destruction of records in archive. Allocate responsibility and oversight for implementation of the plan to Team Leaders or IAO in collaboration with the IGO.		Develop archive plan Implement plan	2017 November 2017 March 2018	M/IGO	
R.13	Create information asset registers for physical and electronic assets storing personal data. Allocate maintenance of the information assets to Team Leaders or IAO. Information assets should be updated, reviewed and risk assessed on a periodic basis.		Ongoing	Work commenced in September 2015 and ongoing. Project due to end March 2017	LDSM/BDIT M/IGO	Blue

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
R.14	It is recommended that the council implement a project plan to ensure future adherence to retention schedules.		Ongoing		LDSM/BDITM/IGO	Blue
R.15	Document the review and weeding process for software systems storing personal data. This task should have an assigned owner and be monitored	Few systems have procedures for removal of personal data currently.	Develop plan for 'weeding' of data as part of R&D work Implementing the plan	September 2017 May 2018	BDITM/Service Managers	Red
R.16	Conduct periodic spot checks of business areas adherence to the clear desk policy. Consider implementing a carding scheme to reflect business areas compliance with the clear desk policy. A carding scheme involves spot checking employee desks after office hours and leaving a green card if the desk is clear of all personal data, an amber card if limited personal data is found or a red card if significant or sensitive personal data is	Clear desk is not presently implemented in many service areas and there is no formal policy to do so, other than a reference to it in the IT Security Policy. We have considered the carding scheme and have no resources at the moment, however it can be included in the Management plan as a desirable action	• Review impacts of implementing clear desk policy • Provide necessary equipment/storage for implementation		LDSM/BDITM	Blue

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
	present. This task should be allocated to a senior employee.					
R.17	Minimise the amount of personal data taken offsite and the overnight storage of personal data should be avoided. Where this is unavoidable the staff member should store personal data securely overnight in a locked briefcase, box or cabinet out of sight, inside their home. The council should consider the possibility of using encrypted portable media to collect personal data offsite as this would reduce the risk of personal data being lost or stolen.	IT Security Policies attempt to limit the amount of electronic personal data taken off site, and where necessary to protect the information should it be misplaced. There is no policy currently in place regarding the transfer of paper-based information off-site.	Develop Policy for Paper-based personal data off-site and ensure that it is implemented. Removal Guidance has been drafted and issued to staff on 31/08/16 via the intranet 'Data Protectors' group and directly to Managers in key areas to provide to relevant staff. IGO contacted IAOs where data is taken off site		LDSM/BDITM/IGO	Blue
R.18	Update the Information Security Incident Management Policy to reflect the current breach reporting process. The IGO should establish and maintain an information security breach log. In	There are policies for Information Security Incident Management which need a review DPA Breaches policy is in place and online forms are available and working well. Logs are kept of both types of incident and investigated where necessary.	• Continue to maintain and process logs. • Learn from previous incidents Updated Data Protection Breach		IGO - LDSM	Blue

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
	addition, the council should create an information security breach reporting form for staff to use.		Management policy and developed new breach reporting e-form for staff.			
R.19	Instruct staff to use lockable cabinets in business areas processing sensitive personal data where possible, so that cabinet, pedestal and drawer keys can be kept securely in the same location. Consider introducing key safes that lock with a key pad to eliminate the risk of storing key safe keys insecurely overnight.		Ensure all personal data can we locked away and the keys to the data controlled by managers.		LDSM/BDITM	Blue
R.20	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-	Access requests are authorised by line management. Ad hoc checks of user access are made occasionally	• Continue to review access levels and requests • Review access levels annually or more frequently where required	Ongoing	BDITM/System Administrators	Blue

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
	term absence should be treated as a security incident and reported to the IGO.					
R.21	It is recommended that the council use lockable bins to dispose of confidential waste onsite prior to collection and shredding. This will help to reduce the risk of confidential waste being read or stolen by unauthorised individuals.	Bins are provided, but the bins are not entirely secure for the purpose of protecting the contents of the bins. At time of replacement it will be considered carefully as to finding a solution – no resources to replace bins which are relatively new.	• Increase awareness of use of bins • Assess risk of non-lockable bins • Consider replacing bins	Ongoing	LDSM/BDITM/Comms	Blue
R.22	It is a breach of the seventh data protection principle not to have a contract '*made and evidenced in writing'* with data processors. It is therefore strongly recommended that the council locate or procure a copy of their third party confidential waste disposal contract and ensure that it contains relevant data protection and information security clauses.	A contract is in place with third party disposal companies, both for electronic and paper data	Continue to maintain contracts with third party providers	Ongoing	LDSM	Blue
R.23	It is recommended that		Develop reporting		LDSM/BDIT	Green

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
	the council start to report more extensively on records management and data protection performance. This could be achieved by including records management, DP training statistics and information security breach key performance indicators in the quarterly Performance and Governance Framework Report.		mechanisms for progress on IG.		M/IGO	
R.24	Include an aspect of information management in the 2015-16 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.	Internal audit are involved in reviewing IG processes and have made a number of recommendation over a period of time.	5 days in the IA plan 16/17		LDSM/BDITM	Blue
R.25	Introduce sample monitoring of Customer Service Advisor calls by management. Sample monitoring should include checking that customer identification	Calls are recorded for training and other purposes. Verification checks are at present limited and warrant a review to ensure best practice is adhered to. Review of verification processes was undertaken in the customer services training by IGO and SIRO	• Introduce sample monitoring		Customer Services Manager	Blue

Ref.	Recommendation	Original position	Agreed action, date and owner	Target Date	Responsible	Progress
	and verification questions are asked when appropriate. Sample monitoring will help to ensure the quality and consistency of the customer experience and reduce the risk of inappropriate disclosures of personal data.					
R.26	Information should be physically secured to ensure that data cannot be removed, stolen or lost. Premises and procedures should be reviewed	IGO has undertaken training in this respect.	• Provide guidance to staff • Check physical security measure adequate at all locations • Provide lockable stores where required • Provide data electronically off-site to reduced likelihood of data loss		LDSM/BDITM/IGO	Blue
R.27	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.	Some ISA's already in place, but not clear whether they are adequate of being adhered to.	Review of existing and required agreements. A database of existing ISA's has been created.		LDSM	Blue