

Action and completion status	Agreed Action	Owner:	Due by	progress
A02	The Data Protection Policy, Information Security Management Policy and Records Management policy reviewed on an annual basis. Any changes to be communicated via Beacon.	SIGO	Apr-16	Review of Policies Complete awaiting approval and communication to staff
A03	Ensure the induction checklist is completed within two weeks of employment for new staff (see also b12).	SIGO	Jan-16	Complete
A04	Amend the Service Area induction checklist to include the requirement to read the Records Management Policy and Information Security Policy.	Training Design & Delivery Manager	Mar-16	Not Complete - Waiting for policies to be approved
A05	Review guidance documentation promoting data protection compliance and review periodically thereafter.	SIGO	Dec-16	Staff IG Handbook completed addition guidance to be considered
A06	Finalise, publish & communicate the toolkit documents	SIGO & Internal Communication	Apr-16	Handbook/Toolkit document awaiting approval and communication to staff
A08	Appoint SIGO and second IGO	Legal services Manager	Jan-16	completed- SIGO - 29/03/16; Second IGO Nov 2015
A12	Set out duties and responsibilities of SIRO and formally reference in relevant policies.	SIGO	Apr-16	Draft completed waiting for approval. Incorporated in policies reviewed so far
A13	Identify IAOs, set out duty's and responsibilities of IAOs and communicate to IAOs, reference role/responsibly within relevant policies & procedures.	SIGO	Sep-16	Roles to be incorporated in risk management policy, staff hand book and IG Toolkit after completion of IAR
A14	Recruit Records Manager or the duties are assigned to an appropriate role/roles	Legal services Manager/ Programme	Jul-16	To consider recruiting
A16	Draft Terms of reference for the IMSG for approval by the group.	Legal Services Manager	Jan-16	Completed but not approved by group

Action and completion status	Agreed Action	Owner:	Due by	progress
A17	Create action plan to ensure key deliverables with Information Management- Bringing it together document are achieved.	SIGO & Programme Manager Transformation	Apr-16	Completed
A18	Draft an Information Risk Policy	SIGO	Sep-16	After IAR has been completed
A19	Ensure that information asset register is up to date and that is regularly reviewed to identify residual risks which require escalations.	SIGO/ Transformation delivery programme Manager	Apr-16	Information asset register has been developed but risk management approach yet to be developed
A20	Create information risk register to capture, record & track information related to risks identified via the IAR, security incidents & PIAs.	SIGO/ Head of ICT Strategy	Sep-16	Not began - after completion of information risk policy
A21	Information Risk register to be considered by SMB.	SIRO	Sep-16	Not began - after completion of information risk policy and Information Risk Register
A22	IMSG to approve Information Risk Register and review on a quarterly basis.	SIRO	Sep-16	Not began - after completion of information risk policy and Information Risk Register
A25	To follow up on data protection audit in 2013/14. To include specific data protection audits within the audit plan 2015/16 & future audit plans.	Chief Internal Auditor	Feb-16	In the process of producing the Audit plan
A26	To include data protection/Information governance control issues within the Annual Governance Statement.	Chief Internal Auditor	Apr-16	Completed

Action and completion status	Agreed Action	Owner:	Due by	progress
A27	SIGO to conduct periodic spots checks to monitor compliance with information governance policies and results to be reported to ISMG.	SIGO	Apr-16	Not began - after completion of policies and procedures
A28	To include statistics in relation to information security incidents & training completion within annual report.	SIGO	Sep-16	Security incidents and training completion being monitored
A29	IMSG to monitor KPIs re completion statistics, training completion & information security incidents on quarterly basis.	Legal services Manager/ SIGO	Implemented November 2015	completed
A31	a) Communicate the requirement for staff to carry out mandatory PIAs for any new service or change in service which involves the processing of personal data to all senior Managers. b) Amend the responsibilities for Line Managers document within the toolkit to include the requirement for mandatory PIAs.	a) SIRO/ b) Legal services manager	Implementation date: a) January 2016. b) Implementation date: Document amended December 2015.	Completes but not yet approved and communicated re IG Staff Handbook
A33	Introduce PIA template based on ICO's Conducting Privacy Impact Assessments Code of Practice.	SIGO	Jun-16	Completed awaiting approval
A34	SIGO to be a signatory to all PIA's and register of PIA's to be maintained.	SIGO	Jun-16	Completed awaiting approval
B01	Include responsibility for ensuring that staff are adequately trained in relation to data protection to the roles & responsibilities of the SIRO.	SIGO	Apr-16	Completed. Awaiting for approval
B02	Oversight of data protection training to be included within the Terms of Reference for the IMSG.	Legal Services Manager	Jan-16	Waiting for IMSG approval

Action and completion status	Agreed Action	Owner:	Due by	progress
B03	IMSG to approve content of training and monitor training statistics to ensure that training is being completed.	SIGO	Jun-16	Training being monitored
B04	SIGO to report on training completion statistics to IMSG on a quarterly basis.	SIGO	Implemented November 2015	Monitoring reports from learning and development
B05	SIGO to conduct a training needs analysis for members of the Information Governance Team.	SIGO	Aug-16	In progress- to be completed with LSM
B08	Amend DP E-Learning to include a module on Subject Access requests.	SIGO/ Training Design & Delivery Manager	Jun-16	Training developed but not yet part of the E learning module
B09	Review & consolidate the e-learning and classroom based modules to ensure all key data protection learning elements are delivered to all relevant staff.	SIGO/ Training Design & Delivery Manager	Jun-16	Completed training included in training matrix. Additional training needs to be included
B12	<p>Recommendation partially accepted.</p> <p>1) Communication to all senior managers that DP E- Learning must be completed by all new employees within 2 weeks of commencing employment.</p> <p>2) Responsibilities for Line Managers document within toolkit to be amended to include requirement that new starters complete DP E-learning within 2 weeks of commencing employment.</p> <p>3) Induction Checklist to be amended to include the requirement to complete the DP E-learning within 2 weeks of commencing employment.</p>	<p>1) SIRO</p> <p>2) Legal Services Manager</p> <p>3) Training Design &amp; Delivery Manager</p>	<p>1) January 2016</p> <p>2) Amendment made December 2015</p> <p>3) March 2016</p>	Toolkit/handbook requires completion and approval

Action and completion status	Agreed Action	Owner:	Due by	progress
B13	IMSG to consider conducting data protection refresher training on an annual basis following amendment to training as above.	IMSG		To be considered
B14	Include requirement to complete mandatory e-learning training & condensed mandatory training within Data Protection Policy.	SIGO	Aug-16	Data Protection Policy reviewed
B16	Develop specific training for IAO's, SARs, handlers and staff involved in data sharing - Also "Recording with care training"	SIGO/ Training Design & Delivery Manager	Aug-16	In progress- to be completed after relevant policies and procedures have been completed. Adhoc training underway
B17	As part of training needs analysis at recommendation B6 to arrange for IGOs to attain BCS Certificate in Data Protection.	SIGO	Apr-16	Training identified Sept to Oct 2016
B18	Information regarding staff who have not completed the DP training to be provided to SMB & cascaded to all managers on a quarterly basis.	SIGO/SIRO	Apr-16	Reports being created
B20	Training completion statistics to be reported quarterly to IMSG.	SIGO	Implemented November 2015	Being reported
B22	Refresh & re-launch Don't Gamble with Data Campaign to launch the 'toolkit.'	SIGO/ Internal Communication s officer	Sep-16	After training has been developed
C01	SIGO to be a signatory on all Data Sharing Agreements and to maintain a register of all DSA's. All DSA's to be reviewed annually. SIGO to report IMSG on DSA Agreements and Reviews on a quarterly basis.	SIGO	Dec-16	Process included in the IG Staff handbook and procedure has been developed. DSAs yet to be reviewed but new ones being logged

Action and completion status	Agreed Action	Owner:	Due by	progress
C02	SIGO to conduct periodic spot checks across the council to ensure that systematic data sharing decisions are being recorded on relevant case files.	SIGO	Aug-16	After completion of IAR/IRR and DSA register
C05	Amend the DP E-learning training to include basic guidance on data sharing.	SIGO	Jun-16	Content included in refresher training to be added to DP E-Learning training
C06	Develop specific training for those with Data Sharing responsibilities with a requirement that such training is completed every 2 years.	SIGO/ Training Design & Delivery Manager	Aug-16	Data Sharing content being developed
C07	1) Action: Amend Data Protection policy to include summary of key points in respect of data sharing & one- off disclosures. 2) Action: Draft data sharing policy and Guidance in accordance with ICO Data sharing code of practice.	1) SIGO 2) SIGO	1) April 2016 2) July 2016	In staff handbook awaiting approval and communication
C09	1) Draft corporate privacy notice to be published on website. 2) Review fair processing notices used throughout the council.	1) SIGO 2) SIGO	1) April 2016 2) December 2016	Partially complete
C10	Draft consolidated fair processing notice for website.	Legal Services Manager	Feb-16	Partially complete
C11	Undertake a review of all DSA's to ensure the incorporate fair processing, consent & exemptions where relevant.	SIGO	Sep-16	Complete waiting for approval
C12	Undertake a review of all DSA's to ensure they cite applicable conditions for fair processing or exemptions.	SIGO	Sep-16	Not began waiting for approval of DSA templates and procedure
C13	Review all DSAs to ensure that it is a requirement to record that consent has been obtained/overridden & why.	SIGO	Sep-16	Not began waiting for approval of DSA templates/policy and procedure

Action and completion status	Agreed Action	Owner:	Due by	progress
C15	Review all consent forms to ensure that they explain circumstances in which personal data may be shared without consent and that consent may be withdrawn.	SIGO	Sep-16	Yet to identify where consent forms have been completed
C17	Include within the Data Sharing Policy requirement that PIA completed in relation to all DSAs.	SIGO	Jul-16	Included in staff handbook
C18	Awareness of Corporate PIA template to be raised through Don't Gamble with Data Campaign & Data sharing policy.	SIGO	Jul-16	After approval of template
C19	Review CISP to ensure it remains fit for purpose & clarify whether data controllers who are not signatories to it but wish to enter into a DSA are required to become signatories to CISP or confirm adherence to it.	SIGO	Sep-16	No began
C20	Publish DSA template on intranet.	SIGO	Jul-16	Waiting for IMMSG approval
C21	Review all DSAs to ensure compliance with ICO Data Sharing Code of Practice.	SIGO	Sep-16	Only current DSA reviewed older other to be reviewed once templates are approved
C23	Amend DSA template to incorporate statement of compliance and include in existing DSAs on review.	SIGO	Sep-16	Included in reviewed template. This will be used to review existing DSAs
C24	SIGO to be added as a signatory to all DSAs and to ensure that all signatory sections are completed prior to being logged on central list.	SIGO	Sep-16	Templates reviewed, waiting for approval
C25	DSAs to be reviewed on annual basis/ SIGO to keep record of review dates and dates completed.	SIGO	Sep-16	Review dates incorporated in DSA register

Action and completion status	Agreed Action	Owner:	Due by	progress
C26	SIGO to maintain a register of all DSAs to be reviewed bi-annually by IMMSG.	SIGO	Sep-16	Developed new Information Sharing and PIA register for new ISA with annual review dates built in. Process yet to be refined.
C27	Include within Data Sharing Guidance, requirements of Government security classifications. Requirement to use classification to be incorporated into DSAs.	SIGO	Sep-16	Included in staff handbook
C28	Revise DSA template to provide clarity as to which sections need to be amended to provide specific details.	SIGO	Sep-16	Draft document in table format with white spaces to indicate areas where more information is required.
C30	As part of review of DSAs, ensure current methods of sharing information captured.	SIGO	Sep-16	in draft document
C31	As part of review of DSA, ensure they specify relevant job roles/teams at each organisation that will be responsible for sharing/processing data and include specific contact details that will be used for sharing information	SIGO	Sep-16	in draft document
C33	As part of review of DSAs, ensure that they should specify what steps should be taken to report, investigate and resolve incidents	SIGO	Sep-16	in draft document
C34	As part of review of DSAs, ensure the relevant job roles and contact details for incident management leads are included	SIGO	Sep-16	in draft document
C36	Ensure that all DSAs record whether data to be shared is factual/opinion and to distinguish between the two.	SIGO	Sep-16	in draft document
C37	Amend DSA template and all existing DSAs to ensure that parties inform each other when shared data has been amended or updated.	SIGO	Sep-16	in draft document



Action and completion status	Agreed Action	Owner:	Due by	progress
C38	Amend the DSA template and existing DSAs to ensure they contain specific provisions re ensuring the quality of the data shared	SIGO	Sep-16	in draft document
C39	Define and document retention periods within DSA and ensure relevant managers record on data controllers system	SIGO	Sep-16	in draft document
C40	Amend DSA template and all existing DSAs to include disposal dates for the shared data	SIGO	Sep-16	in draft document
C41	Amend DSA template and all existing DSAs to contain specific provisions re organisations providing assurance of disposal to each other	SIGO	Sep-16	in draft document
C42	Draft procedure for dealing with one-off requests for disclosure, to be promoted via Beacon, Don't Gamble with Data Campaign	SIGO	Dec-16	Not began
C43	Ensure that procedure for third party requests for information are received in writing	SIGO	Dec-16	Not began
C45	Within Procedure for dealing with third party requests for information, build in requirements for conforming identity of requesters	SIGO	Dec-16	Not began
C47	Create a single corporate log for all one -off requests for disclosure, identity of requestor, exemptions, tracking information	SIGO	Dec-15	Not began
C48	SIGO to report to IMMSG on a quarterly basis the number of one-off requests for disclosure	SIGO	Dec-15	Not began
C49	SIGO to carry out "spot- checks" on the quality of one-off disclosures to ensure quality assurance.	SIGO	Dec-16	Not began

Recommendations/Actions	Number of Actions	Not begun	In progress	Completed
Policies and Procedures	24	8	11	5
DPA Training and Awareness	15	1	11	3
Information Sharing	38	11	17	0
<b>Total</b>	<b>77</b>	<b>20</b>	<b>39</b>	<b>8</b>

