Action and completion status	**Agreed Action**	**Owner:**	**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	Completed
A03	Ensure the induction checklist is completed within two weeks of employment for new staff (see also b12).	SIGO	Completed
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	Completed
A05	Review guidance documentation promoting data protection compliance and review periodically thereafter.	SIGO	Staff IG Handbook completed addition guidance to be considered
A06	Finalise, publish and communicate the toolkit documents	SIGO & Internal Communications Officer	IG Handbook launched
A08	Appoint SIGO and second IGO	Legal services Manager	completed- SIGO - 29/03/16; Second IGO Nov 2015
A12	Set out duties and responsibilities of SIRO and formally reference in relevant policies.	SIGO	Completed
A13	Identify IAOs, set out duty's and responsibilities of IAOs and communicate to IAOs, reference role/responsibly within relevant policies & procedures.	SIGO	Roles incorporated in risk management policy, staff hand book and IG Toolkit after
A14	Recruit Records Manager or the duties are assigned to an appropriate role/roles	Legal services Manager/ Programme	Interim Records Manager in post
A16	Draft Terms of reference for the IMSG for approval by the group.	Legal Services Manager	Completed

A17	Create action plan to ensure key deliverables with Information Management- Bringing it together document are achieved.	SIGO & Programme Manager Transformation	Completed
A18	Draft an Information Risk Policy	SIGO	Complete. Signed off by IMSG on 27th January
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	Information asset register has been developed and placed under ownership of the Records Manager to maintain ongoing.
A20	Create information risk register to capture (IRR) , record and track information related to risks identified via the IAR, security incidents and PIAs.	SIGO/ Head of ICT Strategy	IRR now compiled, and tracking mechanism in place for Asset Owners to update on quarterly basis.
A21	Information Risk register to be considered by SMB.	SIRO	IRR complete and awaiting signoff alonside Information Risk Policy. Approved on 26th January by IMSG and will now go to SMB
A22	IMSG to approve Information Risk Register and review on a quarterly basis.	SIRO	IRR Approved at IMSG on the 27th January 2017
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	Now scheduled. Included in audit plan approved by Audit committee in October 2016
A26	To include data protection/Information governance control issues within the Annual Governance Statement.	Chief Internal Auditor	Completed
A27	SIGO to conduct periodic spots checks to monitor compliance with information governance policies and results to be reported to ISMG.	SIGO	Being conducted on a continual and ad hoc basis
A28	To include statistics in relation to information security incidents and training completion within annual report.	SIGO	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	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	Included in IG handbook and relevant policies
A33	Introduce PIA template based on ICO's Conducting Privacy Impact Assessments Code of Practice.	SIGO	Completed
A34	SIGO to be a signatory to all PIA's and register of PIA's to be maintained.	SIGO	Completed
B01	Include responsibility for ensuring that staff are adequately trained in relation to data protection to the roles and responsibilities of the SIRO.	SIGO	Completed
B02	Oversight of data protection training to be included within the Terms of Reference for the IMSG.	Legal Services Manager	Completed
B03	IMSG to approve content of training and monitor training statistics to ensure that training is being completed.	SIGO	Training being monitored
B04	SIGO to report on training completion statistics to IMSG on a quarterly basis.	SIGO	Monitoring reports from learning and development
B05	SIGO to conduct a training needs analysis for members of the Information Governance Team.	SIGO	Completed and relevant training completed, ongoing or scheduled
B08	Amend DP E-Learning to include a module on Subject Access requests.	SIGO/ Training Design & Delivery Manager	Complete
B09	Review and 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	In progress

B12	Recommendation partially accepted. **1)** Communication to all senior managers that DP E- Learning must be completed by all new employees within 2 weeks of commencing employment. **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. **3)** Induction Checklist to be amended to include the requirement to complete the DP E-learning within 2 weeks of commencing employment.	**1)** SIRO **2)** Legal Services Manager **3)** Training Design & Delivery Manager	Completed
B13	IMSG to consider conducting data protection refresher training on an annual basis following amendment to training as above.	IMSG	Agreed
B14	Include requirement to complete mandatory e-learning training and condensed mandatory training within Data Protection Policy.	SIGO	Completed
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	Complete
B17	As part of training needs analysis at recommendation B6 to arrange for IGOs to attain BCS Certificate in Data Protection.	SIGO	Completed
B18	Information regarding staff who have not completed the DP training to be provided to SMB and cascaded to all managers on a quarterly basis.	SIGO/SIRO	Completed. Dashboard now being developed for CLT
B20	Training completion statistics to be reported quarterly to IMSG.	SIGO	Being reported
B22	Refresh & re-launch Don't Gamble with Data Campaign to launch the 'toolkit.'	SIGO/ Internal Communications officer	IG Handbook completed- launch date 20/10/2106
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	SIGO	Process included in the IG Staff handbook and procedure has been developed.
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	Complete and now ongoing

C05	Amend the DP E-learning training to include basic guidance on data sharing.	SIGO	Complete. Content included in refreshed 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	Data Sharing content 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**	Completed
C09	**1)** Draft corporate privacy notice to be published on website. **2)** Review fair processing notices used throughout the council.	**1)** SIGO **2)** SIGO	Completed
C10	Draft consolidated fair processing notice for website.	Legal Services Manager	Completed
C11	Undertake a review of all DSA's to ensure the incorporate fair processing, consent & exemptions where relevant.	SIGO	All Key DSAs now reviewed but ongoing action now identified to look at any other via the new IAR
C12	Undertake a review of all DSA's to ensure they cite applicable conditions for fair processing or exemptions.	SIGO	All Key DSAs now reviewed but ongoing action now identified to look at any other via the new IAR
C13	Review all DSAs to ensure that it is a requirement to record that consent has been obtained/overridden and why.	SIGO	All Key DSAs now reviewed but ongoing action now identified to look at any other via the new IAR
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	All Key DSAs now reviewed but ongoing action now identified to look at any other via the new IAR
C17	Include within the Data Sharing Policy requirement that PIA completed in relation to all DSAs.	SIGO	Completed
C18	Awareness of Corporate PIA template to be raised through Don't Gamble with Data Campaign & Data sharing policy.	SIGO	Completed

C19	Review CISP to ensure it remains fit for purpose and clarify whether data controllers who are not signatories to it but wish to enter into a DSA are required to become signatories to CISP of confirm adherence to it.	SIGO	Action may have been superseded and should a new protocol be required it can be shorter and less specific, but complemented by specific data sharing agreements with partners
C20	Publish DSA template on intranet.	SIGO	Completed
C21	Review all DSAs to ensure compliance with ICO Data Sharing Code of Practice.	SIGO	All Key DSAs now reviewed but ongoing action now identified to look at any other via the new IAR
C23	Amend DSA template to incorporate statement of compliance and include in existing DSAs on review.	SIGO	Completed
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	Ongoing
C25	DSAs to be reviewed on annual basis/ SIGO to keep record of review dates and dates completed.	SIGO	Review dates are incorporated within the DSA register
C26	SIGO to maintain a register of all DSAs to be reviewed bi-annually by IMSG.	SIGO	Ongoing
C27	Include within Data Sharing Guidance, requirements of Government security classifications. Requirement to use classification to be incorporated into DSAs.	SIGO	Completed
C28	Revise DSA template to provide clarity as to which sections need to be amended to provide specific details.	SIGO	Completed
C30	As part of review of DSAs, ensure current methods of sharing information captured.	SIGO	All Key DSAs now reviewed but ongoing action now identified to look at any other via the new IAR
C31	As part of review of DSA, ensure they specify relevant job roles/teams at each organisation that will be responsible for	SIGO	All Key DSAs now reviewed but ongoing action now identified to
C33	As part of review of DSAs, ensure that they should specify what steps should be taken to report, investigate and resolve incidents	SIGO	All Key DSAs now reviewed but ongoing action now identified to look at any other via the new IAR

C34	As part of review of DSAs, ensure the relevant job roles and contact details for incident management leads are included	SIGO	All Key DSAs now reviewed but ongoing action now identified to look at any other via the new IAR
C36	Ensure that all DSAs record whether data to be shared is factual/opinion and to distinguish between the two.	SIGO	All Key DSAs now reviewed but ongoing action now identified to look at any other via the new IAR
C37	Amend DSA template and all existing DSAs to ensure that parties inform each other when shared data has been amended or updated.	SIGO	All Key DSAs now reviewed but ongoing action now identified to look at any other via the new IAR
C38	Amend the DSA template and existing DSAs to ensure they contain specific provisions re ensuring the quality of the data shared	SIGO	All Key DSAs now reviewed but ongoing action now identified to look at any other via the new IAR
C39	Define and document retention periods within DSA and ensure relevant managers record on data controllers system	SIGO	All Key DSAs now reviewed but ongoing action now identified to look at any other via the new IAR
C40	Amend DSA template and all existing DSAs to include disposal dates for the shared data	SIGO	All Key DSAs now reviewed but ongoing action now identified to look at any other via the new IAR
C41	Amend DSA template and all existing DSAs to contain specific provisions re organisations providing assurance of disposal to each	SIGO	All Key DSAs now reviewed but ongoing action now identified to
C42	Draft procedure for dealing with one-off requests for disclosure, to be promoted via Beacon, Don't Gamble with Data Campaign	SIGO	Completed
C43	Ensure that procedure for third party requests for information are received in writing	SIGO	Completed
C45	Within Procedure for dealing with third party requests for information, build in requirements for confirming identity of requesters	SIGO	Completed
C47	Create a single corporate log for all one -off requests for disclosure, identity of requestor, exemptions, tracking information	SIGO	Completed

C48	SIGO to report to IMSG on a quarterly basis the number of one-off requests for disclosure	SIGO	Completed
C49	SIGO to carry out "spot- checks" on the quality of one-off disclosures to ensure quality assurance.	SIGO	Included in work plan and have already checked on CCTV and WA170 requests procedure

	Jun-16	Oct-16	Feb-17
Red (No significar	20	4	0
Amber (On-going	49	27	2
Green (Complete	8	46	75