APPENDIX B: IAO: IG & GDPR Management Plan

V 2.0 July 2017

Ref.	Recommendation	Agreed action, date and owner	Responsible	Review Period	Next review due
Governance					
T.11	Consider incorporating data protection as a regular agenda item at team meetings.	Agree level for Data Protection issues to be discussed e.g. DMT/SMTs	LDSM/BDITM	Quarterly	September 2017
Records Management					
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.	Remind IAOs of obligations	LDSM/BDITM/IGO/Managers	Annually	September 2017
R.10	Review Privacy Notices	Carry out period reviews	LDSM/IGO	Quarterly	September 2017
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	LDSM/BDITM/IGO		September 2017
R.14	It is recommended that the council implement a project plan to ensure future adherence to retention schedules.	Review plan	LDSM/BDITM/IGO	Quarterly	September 2017
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 present. This task should be allocated to a senior employee.	Remind officers of obligations and spot check	LDSM/BDITM/IGO	Annually/Adhoc	September 2017
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.	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	Quarterly	September 2017

Ref.	Recommendation	Agreed action, date and owner	Responsible	Review Period	Next review due
R.18	DP Breach Management policy	monitor through IG group and officers for lessons learnt and trends	LDSM/BDITM/IG Group	Quarterly	September 2017
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.	Remind IAOs of obligations	LDSM/BDITM	Annually	September 2017
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-term absence should be treated as a security incident and reported to the IGO.	Review Access Levels	BDITM/System Administrators	Annually	September 2017
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.	Review disposal procedures	LDSM/BDITM	Annually	September 2017
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.	Review third party contracts	LDSM	Annually	September 2017
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.	Review Audit requirement	LDSM/BDITM	Annually	September 2017
R.25	Introduce sample monitoring of Customer Service Advisor calls by management. Sample monitoring should include checking that customer identification 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.	Monitor sampling of calls	Customer Services Manager	Adhoc	September 2017

Ref.	Recommendation	Agreed action, date and owner	Responsible	Review Period	Next review due
R.26	Information should be physically secured to ensure that data cannot be removed, stolen or lost. Premises and procedures should be reviewed	Review Physcial security of data, on and off site	LDSM/BDITM/IGO	Annually	September 2017
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	Review of existing and required agreements. A database of existing ISA's has been created.	LDSM	Quarterly	September 2017

PLEASE NOTE:

The review date has been moved to September 2017 as the Information Asset Owner Handbook will be rolled out by then and covers these areas.