Risk Driven Action Plan– Essential Reference Paper ‘B’

Corporate Level Risks

Observations	Risks	Actions
Inconsistent application of the Council’s document retention and disposal policy.	Risk of a breach of DP Principles4and 5.	**Risk has been assessed with reference to Data Security.** **Off-site storage of documents has been assessed, and is likely to require considerable resource to resolve. Current process of archive management devolved to service level offers little oversight and while some service hold excellent records, work needs to be undertaken to ensure that stored documents are disposed of when no longer required.** **Ware storage site remains a considerable concern. Suggest that work be undertaken to review all material stored there.** **Electronic retention is considered to be lower risk due to very good IT security protocols, but new systems should be procured with retention/deletion of records a consideration.**
Inconsistent use of ‘fair processing’ notices.	Risk of a breach of DP Principles 1and6.	**Continued use existing opportunities such as staff briefings and Team Update to improve awareness of the issues.** **Review forms and collection notices as part of service level content development project.** **Information Management team empowered to audit services’ compliance with the policy, to be undertaken through service level content development project.** **Support through DP reviews as part of Service Planning** **Operational Risk Management Group to review audits and make recommendations to SMG/CMT where considered appropriate.**
Inconsistent approach to data sharing.	Risk of a breach of DP	**Continued use existing opportunities such as staff briefings and**

	Principles2, 6 and 7.	**Team Updateto improve awareness of the issues.** **Ongoing targeted support for staff and services involved in Data Sharing.** **Information Management team empowered to audit services’ compliance with the policy.** **Support through DP reviews as part of Service Planning** **Operational Risk Management Group to review audits and make recommendations to SMG/CMT where considered appropriate.**

Service Based Risks

1. Revenues and Benefits

Observations	Risks	Recommendations
Revenues ‘Fair collection’/‘privacy notices’ must be in place on all documents and web forms where personal data are collected.	Risk of a breach of DP Principles1 and6.	Ensure ‘fair collection’ / ‘privacy notices’ in place on all documents and web forms where personal data are collected.**Reviewed and agreed to be compliant**
Occasional data sharing takes place (police).	Risk of a breach of DP Principles 2, 6 and 7	Ensure all acts of data sharing are legitimate under the terms of the DPA and appropriately logged.**Ongoing support, but compliant**
Third party organisation used to process personal data on behalf of the service. Occasional use of temporary staff.	Risk of a breach of DP Principles 2, 6 and 7	Ensure mandatory (and if appropriate optional), DP clauses are built into contract and compliance monitored. Ongoing support, but compliant Ensure temporary/agency staff receive DP training and compliance is monitored.**Ongoing support, but compliant**
Benefits ‘Fair collection’ / ‘privacy notices’ must be in place on all documents and web forms where personal data are collected.	Risk of a breach of DP Principles1 and 2.	Ensure ‘fair collection’ / ‘privacy notices’ in place on all documents and web forms where personal data are collected. **Reviewed and agreed to be compliant**
Occasional data sharing takes place (police).	Risk of a breach of DP	

	Principles 2, 6 and 7	Ensure all data sharing is legitimate under the terms of the DPA and are appropriately recorded.**Ongoing support, but compliant**

2. Communications, Engagement and Cultural Services

Observations	Risks	Recommendations
Personal data of competition winners and of other newsworthy individuals may be publicised by the section.	Risk of breach of DP Principles 1 and 5.	Ensure that the consent of the individual is obtained and a record held on file.**Ongoing support, but compliant**
Individuals who sign up for aspects of the service have that service delivered through "GovDelivery".	Risk of breach of DP Principles 1 and 7.	Ensure an appropriate 'Privacy Statement' is made available to the individual and that appropriate DP clauses are present in any agreement between EHDC and 'GovDelivery'. **Ongoing support, but compliant**
No significant, unmanaged DP risks identified in the areas of Hertford Theatre and Engagement and Partnerships.	N/A	Risks identified during the review process were largely resolved during the year.**Ongoing support, but compliant**

3. Finance and Performance

Observations	Risks	Recommendations
No significant, unmanaged DP risks identified in course of review.	N/A	Ensure appropriate security of mechanisms by which personal data are transferred to and from the Finance and Performance team and other services. **Ongoing support, but compliant**

4. Payroll/HR

Observations	Risks	Recommendations
Employees are asked to update their personal data on a two year cycle.	Risk of breach of DP Principle 4.	Update on a more frequent basis (perhaps update a twelfth of the workforce each month, in a yearly cycle?).**The new HR system planned for implementation this year will allow for immediate update of**
Some employee personal data is held in	Risk of breach of DP Principle 7.	

physical form (i.e. files). Payroll processing is externalised. HR co-ordinates delivery of most corporate level training and guidance.	 Risk of breach of DP Principle 7. N/A	**information and employees would be encouraged to do this.** Ensure physical security of files. Consider additionallevels of security in respect of any *sensitive* personal data contained in files.**Ongoing support, but compliant** Ensure requisite DP clauses are present in contract/SLA with external processor and, as appropriate, with SBC.**Ongoing support, but compliant** Ensure DP training takes place at induction and on a regular basis and that the delivery of this training is logged. Follow-up action is taken in respect of those who fall through the net**. Induction process has been reviewed and mentions DP in corporate induction and referral to pages on the intranet are made** Ensure Staff Handbook is updated on a periodic basis and made accessible to staff. Liaise with Information Management team to ensure accuracy of DP statements in the Handbook.**Staff Handbook has been updated this year and goes to HR Committee in July 2015**

5. Facilities and Property Management

Observations	Risks	Recommendations
Service may occasionally receive requests for personal data from the Police.	Risk of breach of DP Principles 2, 6 and 7.	Although S29 of the DPA sets out the basis on which personal data may be shared with bodies such as the Police, fundamental requirements remain, such as the need to establish a legitimising condition. Data sharing practices and protocols between EHDC, the police and other enforcement authorities should be reviewed at a corporate level, to ensure they are robust and fit-for-purpose. **Requests are managed via DMI team Ongoing support, but compliant**

Service has responsibility for some CCTV recording at Wallfields and Charrington's House.	Risk of breach of DP Principles 1, 2, 5, 6, 7.	Ensure an appropriate 'Code of Conduct' is in place and reviewed on a periodic basis. Ensure appropriate procedure is in place to manage Subject Access Requests and requests for data sharing from other agencies (see above).**Access requests managed through DMI team, Code of Conduct under review**

6. Corporate Risk

Observations	Risks	Recommendations
No significant, unmanaged DP risks identified in course of review.	N/A	Measures are in place to legitimise and manage the service's key activities, including in potentially sensitive areas such as fraud prevention/detection. It is vital that detailed records are kept when activities such as investigations/covert monitoring take place and that senior management authority is secured and recorded where appropriate**. Compliant and V High levels of Assurance**

7. Licensing and Community Safety

Observations	Risks	Recommendations
Community Safety and Health Services Substantial volumes of personal and sensitive personal data may be collected as part of this function.	Risk of breach of DP Principles 1, 3, 4, 5, 6, 7	Ensure 'fair processing' information is given as close as possible in time to when personal data are collected, whatever the medium used, and that it is provided in an appropriate format. **Ongoing support and review – compliant in many core areas, but the service seeks further corporate support** Ensure data sharing agreements are in place with organisations with whom personal data may be shared and ensure the security of all channels by which the data sharing may take place.**Ongoing support, but compliant** Ensure the service retains and disposes of personal data in line with

Risk Driven Action Plan– Essential Reference Paper ‘B’

		corporate policy.**Retention remains a concern in regard of electronic data: security is good, but electronic disposal is not possible.**
ASB Case Management Substantial volumes of personal and sensitive personal data may be collected as part of this function.	Risk of breach of DP Principles 1, 3, 4, 5, 6, 7	Ensure ‘fair processing’ information is given as close as possible in time to when personal data are collected, whatever the medium used, and that it is provided in an appropriate format **Ongoing support and review – compliant in many core areas, but the service seeks further corporate support** Ensure data sharing agreements are in place with organisations with whom personal data may be shared and ensure the security of all channels by which the data sharing may take place.**Ongoing support, but compliant** Ensure the service retains and disposes of personal data in line with corporate policy. **Retention remains a concern in regard of electronic data but security is good,**
Safety Advisory Group Personal data is processed as part of this Group’s activities and is shared with other members of the SAG.	Risk of breach of DP Principles 1, 3, 4, 5, 6, 7	Ensure ‘fair processing’ information is given as close as possible in time to when personal data are collected, whatever the medium used, and that it is provided in an appropriate format Ensure data sharing agreements are in place with other members of the SAG and ensure the security of all channels by which the data sharing may take place.**Ongoing support, but compliant** Ensure the service retains and disposes of personal data in line with corporate policy.

		Service level DP awareness remains very high, with very good compliance behaviours

8. Democratic Services (including Members)

Observations	Risks	Recommendations
No significant, unmanaged DP risks identified in course of review.	N/A	Member Guidance on DP to be revised and re-issued on a periodic basis.**Ongoing support, but compliant** DP training to be formalised as part of the induction process post local elections.**Ongoing support, but compliant** Additional Member training to be identified and implemented. **Ongoing support, but compliant**

9. Planning and Building Control

Observations	Risks	Recommendations
Personal data, (albeit limited in volume and sensitivity) are gathered as part of the planning and building control process.	Risk of breach of DP Principles 1 and 5	Appropriate 'fair collection' / 'privacy notices' are made available where personal data are collected.**Ongoing support, but compliant**
Personal data may be retained on key systems long after the conclusion of the matter to which it relates. (Appears to be a limitation of the current IT system)	Risk of breach of DP Principle 5	Service should use the opportunity the forthcoming retendering of this system provides to specify an appropriate means of deleting (or at least 'putting beyond use' the personal data of individuals as per the Council's retention and disposals policy.**Retention remains a concern in regard of electronic data but security is good**

10. Corporate Support

Observations	Risks	Recommendations
The team processes significant amounts of	Risk of breach of DP Principle 7.	Review mechanism(s) by which documents containing personal data are

personal data; however it acts primarily as a 'clearing house', disseminating data to and receiving it from, internal departments and outside organisations.		transmitted to and from members of the Corporate Support team. **Ongoing support, but compliant**
The services of an external company are used to process personal data on behalf of the Corporate Support team.	Risk of breach of DP Principles 2, 6 and 7.	Ensure requisite DP clauses are present in contract/agreement between Council and company. **Ongoing support, but compliant**

11. Assets and Estates Management

Observations	Risks	Recommendations
The service conducts credit checks on individuals.	Risk of breach of DP Principle 7.	Consider additional security (e.g. password protection) of the computer files in which this personal data are held.**Ongoing support, but compliant**

12. Customer Services and Parking

Observations	Risks	Recommendations
Customer Services The team processes significant amounts of personal data; however it acts primarily as a 'clearing house', disseminating data to and receiving it from, internal departments and outside organisations.	Risk of breach of DP Principle 7.	Review mechanism(s) by which documents containing personal data are transmitted to and from members of the Corporate Support team. Ensure documents containing personal data are not left exposed to public view – e.g. on desktops in reception areas.**Ongoing support, but compliant**
The service co-ordinates the '3 C's' process (Compliments, Comments and Complaints.	Risk of breach of DP Principle 1.	Ensure 'fair processing' information on relevant documentation is complete, that it acknowledges the individual's right to withhold consent for their personal data to be shared and that the consequences of such a refusal are clearly explained. **Ongoing support, but compliant**

Information Management Web team pre-check most website content before it goes live, but there are a few circumstances where services can post direct.	Risk of breach of DP Principle 1,	Individual services posting personal data to the web must take responsibility for ensuring the legitimacy of doing so. **Ongoing support, but compliant**
Team co-ordinates processing of all FOI and DP inquiries received by the Council.	Risk of breach of DP Principles 6 and 7.	Systems and controls in place within the service make a DP breach unlikely; however training in the identification and proper treatment of Subject Access Requests needs to be given to all services on a periodic basis.**Ongoing support, but compliant**
Parking Services No significant, unmanaged DP risks identified in course of review in respect of the enforcement and permit functions.	N/A	N/A
Risk of DVLA data being retained longer than the purpose for which it was obtained justifies.	Risk of breach of DP Principles 2 and 5.	Explore options to delete redundant personal data from PCN records according to pre-agreed criteria. . **Retention remains a concern in regard of electronic data but security is good**

13. Housing

Observations	Risks	Recommendations
No significant, unmanaged DP risks identified in course of review.	N/A	Risks identified are corporate risks and will be progressed on that basis.

14. Environmental Services (including LeisureServices)

Observations	Risks	Recommendations
General The personal data of staff are processed as part of the service's management of the 'lone	N/A	Ensure staff are given 'fair processing' information at the point the personal data are gathered. **Ongoing support, but compliant**

worker' function. (N.B. Similar arrangements and recommendations will apply in respect of other services; however this was the only review in which the situation was addressed in detail). **Waste Management** No significant, unmanaged DP risks identified in course of review. **Environmental Inspection/Pest Control** No significant, unmanaged DP risks identified in course of review. **Grounds maintenance/TPOs/allotments** No significant, unmanaged DP risks identified in course of review. **Leisure Services** No significant, unmanaged DP risks identified in course of review.	N/A N/A N/A N/A	Ensure a mechanism for reviewing accuracy of personal data on a periodic basis and ensure a mechanism for deleting personal data should an individual leave the Council's employ.**Retention remains a concern in regard of electronic data but security is good** Ensure the physical and electronic security of these data – especially after move towards holding data on PDAs. **Ongoing support, but compliant** N/A N/A N/A N/A

15. IT Services

Observations	Risks	Recommendations
Information Technology risks from service reviews highlighted: Growth in use of bring your own/portable devices Growth in home working Non-secure email	Clear policy revisions required to update and support use of IT equipment.	IT risks have been addressed through a variety of meaures: • deployment of hosted desktop to insulate the network from BYOD (Bring Your Own Device) risk. • Creation of IL3 "bubble" to apply more stringent security policies to users accessing sensitive data. • New IT strategy creating flexible and context sensitive framework.

Risk Driven Action Plan– Essential Reference Paper ‘B’

IT unable to progress risk assessments due to establishment of shared service structure and government changes to local authority IT practices. This now concluded so assessments and policies will be undertaken by July2014.		• New IT policies in draft and proceeding. • Training has been rolled out to staff on email security via “Bob’s Business” e-learning suite. Confidence in IT security is high, with substantial level of assurance from recent audit.