EAST HERTS COUNCIL

CORPORATE BUSINESS SCRUTINY COMMITTEE – 27 MAY 2014

REPORT BY HEAD OF INFORMATION, CUSTOMER AND PARKING SERVICES

DATA PROTECTION ANNUAL REVIEW

WARD(S) AFFECTED: ALL

Purpose/Summary of Report:

- To update the Committee on the implementation of the Council's Data Protection Action Plan.
- To invite the Committee to comment on progress to date.

RECOMMENDATIONS FOR CORPORATE BUSINESS SCRUTINY: That:	
(A)	**The implementation of the Council's Data Protection Action Plan be noted and endorsed; and**
(B)	**The Executive be advised of any recommendations regarding the Council's Data Protection Action Plan.**

1.0 Background

1.1 Following an external audit of the Council's data protection (DP) compliance, Corporate Management Team (CMT) adopted an Information Security Framework and agreed priorities for DP policy development and implementation 25 Sept 2012.

1.2 Governance structures agreed at Corporate Business Scrutiny (CBS) Committee on 19 March 2013 included provision of an annual update for scrutiny by CBS in their governance role (strategic oversight) of the Council's data protection compliance arrangements.

1.3 Data protection breaches occur in the best run organisations. The primary purposes of implementing DP compliance are:

- To ensure DP risks are prioritised and managed.

- To equip officers and Members with the tools they need to promote DP compliance in the course of their work.
- In the unfortunate event of a reportable breach, to demonstrate that the Council had policies and guidance in place that, had they been observed, would have obviated the breach or at least mitigated its severity.

2.0 Report

2.1 Reviews and Risk Assessments

2.1.1 All services undertook DP reviews of key processes in 2013/14 using a template from the Information Management (IM) team. These were analysed and feedback offered. This included recommendations to enhance DP compliance and minimise risk.

2.1.2 The review:

- Enabled services to understand their key business processes, considering them afresh from a DP perspective.
- Equipped services to complete the mandatory DP risk assessment in their 2014/15 Service Plan.
- Enabled the IM team to identify common DP risks and of sufficient import that they should be managed as corporate risks by the Operational Risk Management Group.
- Enabled the IM team to prepare a risk driven action plan to for DP compliance (**Essential Reference Paper 'B'**).

2.1.3 Three corporate risks were identified and reported to CMT on 29 January 2014:

- Application of the document retention and disposal policies
- Use of 'fair processing notices' (privacy notices)
- Data sharing

2.1.4 The IM team will work with services to deliver enhancements that address the corporate and any service-based risks identified.

2.1.5 Key Information Technology (IT) risks identified were:

- Increasing use of portable devices
- Growth in home working
- Use of non-secure email

2.2 Policy Development

2.2.1 CMT adopted a revised DP policy framework on 12 November 2013. Non-IT policies are drafted for final review. Five have human resources implications to be progressed with HR via Local Joint Panel.

2.2.2 IT policy development is led by Shared IT Services. A delay in developing these policies arose from proposed government-imposed changes to local authority IT management practices. Discussions with the Public Sector Network Team at the Cabinet Office have now been concluded and new IT policies will be brought forward for consultation with SMG, Trade Unions and HR Committee in June 2014.

2.3 Staff Handbook and Training

2.3.1 The Staff Handbook is being revised by the IM team and HR to ensure adequate and accurate reference to DP obligations.

2.3.2 Data Protection forms part of the induction programme and all employees are required to complete an online DP training package (tracked by HR). CMT have confirmed this as mandatory on an annual basis.

2.3.3 Where an individual service has identified a DP learning need, they must discuss this with HR to source an appropriate solution in conjunction with advice/recommendation from the IM team.

2.4 Member Guidance

2.4.1 Data Protection Guidance was issued to Members during 2013. Forty-one of fifty Members have confirmed receipt and understanding. The booklet has since been revised and will be incorporated in the Member Handbook and induction process, in advance of the local elections in May 2015.

2.4.2 The Guidance advises Members that by virtue of certain of their activities they are required to register with the office of the Information Commissioner as a Data Controller in their own right. Four out of fifty Members are known to have registered with the ICO.

2.4.3 The IM and HR teams recommend:

- Member Guidance document (as described above) to be

issued annually (and certainly post-election or by-election), with Members required to confirm their receipt and understanding.

- Amend an existing training video, to create a short, online video training resource for Members.
- Create and issue a DP workbook to mirror the online resource for those Members unable to take part in the online training.
- Issue in-year updates through the Members' Information Bulletin.

2.5 Service Based Risks

2.5.1 A number of local risks were identified during the review process, some unique to just one service. These are summarised in the action plan. Services will be re-visited by the IM team to check on their progress with the implementation of recommendations.

2.5.2 With the exception of the three corporate level risks, none of the individual issues identified in the Action Plan are regarded as significant. Additionally, in many service areas DP awareness and compliance is significant and improving.

2.5.2 Heads of Services will re-certificate each year rather than having to repeat a full DP review process if no changes have taken place to their processes. Re-certification will take place around September/October each year as a precursor to services starting preparation of their Service Plans. Should a business process change fundamentally during the year and should this have ramifications for DP compliance, services should undertake a fresh review at that time.

2.6 Other Actions

2.6.1 The following activities have also taken place over the past year:

- Creation of 'Frequently Asked Questions' on the Intranet.
- Revised guidance on the application of 'fair processing' notices (aka 'privacy notices').
- The DP breach reporting form has been made an e-form.
- 'At a glance' guidance has been prepared for the intranet which will help officers when responding to Member requests for information.

2.6.2 A number of services identified current IT systems as a barrier to ideal DP compliance (primarily retention and disposal). As and when such systems are renewed the relative security and accuracy with which personal data are processed and can be 'put beyond use' when appropriate should be made an important criterion in the tendering process.

3.0 Implications/Consultations

3.1 Information on any corporate issues and consultation associated with this report can be found within **Essential Reference Paper 'A'**.

Background Papers

(i) Minutes of the Corporate Business Scrutiny Committee on 19 March 2013
http://online.eastherts.gov.uk/moderngov/ieListDocuments.aspx?CId=143&MId=2095&Ver=4

(ii) Minutes of the Corporate Business Scrutiny meeting on 2 July 2013
http://online.eastherts.gov.uk/moderngov/ieListDocuments.aspx?CId=143&MId=2093&Ver=4

Contact Member: Councillor Tony Jackson – Leader of the Council.
tony.jackson@eastherts.gov.uk

Contact Officer: Neil Sloper – Head of Information, Customer and Parking Services, Extn: 1611.
neil.sloper@eastherts.gov.uk

Report Author: Neil Sloper – Head of Information, Customer and Parking Services, Extn: 1611.
neil.sloper@eastherts.gov.uk