EAST HERTS COUNCIL

CORPORATE BUSINESS SCRUTINY COMMITTEE – 19 MARCH 2013

REPORT BY HEAD OF INFORMATION, CUSTOMER AND PARKING SERVICES

6. DATA PROTECTION AND INFORMATION SECURITY UPDATE

WARD(S) AFFECTED: ALL

Purpose/Summary of Report:

- To provide an update on the Council's management of Data Protection and Information Security
- To invite the Committee to take up a role in the Council's governance framework for Information Security.

RECOMMENDATIONS FOR CORPORATE BUSINESS SCRUTINY COMMITTEE That:	
(A)	The Council's Data Protection Action Plan and Governance Framework be scutinised;
(B)	Corporate Business Scrutiny Committee considers and adopts it's recommended role in the governance arrangements for Data Protection and monitoring the completion of the Data Protection Action Plan;
(C)	A training session to support the governance role of Members of Corporate Business Scrutiny Committee be endorsed; and
(D)	The Executive be advised of any recommendations regarding the Information Security Framework now detailed.

1.0 Background

1.1 Corporate Management Team (CMT) authorised an independent review of Data Protection (DP) across all services on 13 March 2012.

1.2 The review made recommendations regarding DP policies and guidance. CMT approved an Information Security Policy

Framework and the priorities for policy development on 25 September 2012.

1.3 CMT received a DP update report on 13 March 2012. This established basic governance of DP including: Heads of Services' (HOS) responsibility to ensure their teams are aware of the impact and requirements of the DP Act; and alignment of DP risk assessment and review alongside the Council's existing arrangements for managing and monitoring risks.

2.0 Report

2.1 Data Protection Review

2.1.1 An extensive DP review including 16 individual service reports, resulted in an action plan to continue to enhance the Council's approach to managing the requirements of the DP act. This action plan is presented as **Essential Reference Paper B.**

2.1.2 During the review, immediate actions were taken to begin addressing any concerns identified where possible.

2.2 Approach to Information Security

2.2.1 The review identified that:

- The Council had a basic set of DP policies, which can be enhanced to reflect the demands that are now placed on Councils, driven in part by the increased use of information technology.
- The establishment of enhanced policies would also be beneficial by increasing knowledge amongst all staff.
- The establishment of enhanced policies would also increase knowledge amongst all staff.

2.3 Data Protection Policies and Procedures

2.3.1 The existing policies covering DP, were established over time, as needs arose. The Council is now implementing a structured framework under an Information Security policy that reflects best practice. Some specific policies addressing single issues are required. An example is home working. The number of staff 'home working' has grown from fewer than 10 to almost 50. Previously a

small addition to an existing policy was fit for purpose, a more comprehensive policy with guidance is now required.

2.3.2 The order of policy development is based on potential risk to the Council and need. This order is show in **Essential Reference Paper C.** The initial priorities were 'Use of Social Media', now completed, and 'Councillor Guidance', on track for completion by end of March 2013.

2.4 Policies Covering the Computing Environment

2.4.1 East Herts' Systems and Network Manager and its Development Manger have confirmed that a number of policies are required in respect of Information Security and ICT (shown in **Essential Reference Paper C).** CMT have endorsed that the ICT shared service address establish common security policies at an early stage of the project. Specific ICT security policies required in addition to these will then be progressed.

2.5 Monitoring Progress – Governance

2.5.1 The existing Arrangements were approved on 13th March 2012 by CMT:

- A quarterly DP compliance monitoring report to CMT, to ensure prompt and committed progress whilst tracking the completion of DP risk assessments and resulting actions.
- That all Head of Service (HoS) must ensure their teams are aware of the impact of, and their responsibilities under, the DP Act in their service, with assistance and guidance provided by the Information Management team.
- That all services include an annual DP risk assessment as part of the established Medium Term Financial Planning (MTFP) process.
- That Directorate Management Teams (DMTs) will monitor risks and associated actions quarterly with significant matters flagged on the corporate risk register.

2.5.2 The DP action plan recognises the need for enhanced monitoring and governance to ensure a strong level of assurance in compliance with DP requirements. The governance structure is presented in **Essential Reference Paper D.**

2.5.3 East Herts Council's Annual Governance Statement defines the

role of Overview and Scrutiny committees (Corporate Business Scrutiny, Community Scrutiny and Environment Scrutiny) as '*the review and/or scrutiny of decisions made or actions taken in connection with the discharge of any of the Council's functions, developing the capacity and capability of members and officers to be effective*'. Audit Committee provides '*assurance about the adequacy of internal controls, financial accounting and reporting arrangements, and that effective risk management is in place*'.

2.5.4 It is proposed that Corporate Business Scrutiny committee takes a strategic oversight of the completion of the DP action plan and DP compliance with a formal annual report.

2.6 Roles and Responsibilities - Organisation

2.6.1 **Essential Reference Paper D** sets out the DP governance arrangements within the Council as approved by CMT on 13 March. The specific roles and responsibilities are shown with the reporting arrangements in place.

2.6.2 The Chief Executive and Director of Community and Customer Services is the Senior Information Risk Owner (SIRO) with overall ownership of the Council's Information Risk Policy, acting as the champion for information risk on CMT.

2.6.3 The management and responsibility for the implementation of the Council's DP Risk Policy will be given to the Deputy SIRO, the Head of Information, Parking and Customer Services. The post holder will lead the Council's DP compliance and will be a source of challenge and advice on DP matters, standing in for the SIRO as required.

2.7 Data Protection Compliance Officer

2.7.1 In order to deliver efficient and focused change CMT have established a one year post of Data Protection Compliance Officer.

2.7.2 The one year role is required to support the Information Management team and organisation to deliver the Information Security Policy Framework, its sub-policies and the DP Action Plan. The role will ensure:

- Organisational risks will be mitigated swiftly.
- Services will be supported to develop knowledge of information flows, risks and risk mitigation.

- Services will be supported to develop appropriate in-service training to mitigate data protection risks.
- All staff will benefit from the implementation of up to date Data Protection policies that reflect our organisational needs.
- CMT will benefit from the assurance that a dedicated project officer supports the Data Protection Action Plan across the whole organisation.

2.8 Members and Data Protection

2.8.1 Members are covered by the Council's own Data Protection registration with the Information Commissioner whilst undertaking duties as a member of the Council. The Council's training will support members in these roles in respect of Data Protection and Information Security matters. Specific training will be provided to the Licensing Committee due to the nature of their work, Corporate Business Scrutiny due to the proposed governance role and the Executive and political group leaders so they are a source of peer support.

2.8.2 Members are individually responsible and liable under the Data Protection Act if they hold or use and personal data for the purpose of constituency casework or for canvassing political support amongst the electorate. This is likely to be the case for any active Ward Councillor. It is each individual member's responsibility to ensure they have individually complied with the requirements of the Data Protection Act and registered as a Data Controller with the Information Commissioner's Office.

2.8.3 The Member Development Charter Group agreed that essential training for members be offered in the format of:

- An induction pack/Introductory Guide to Data protection for Members
- Essential e-learning for Members on Data Protection and Information Security, both backed up with hard copy workbooks as an alternative by exception where e-learning is not the best format for learning
- Additional information for Members to be highlighted on the Member intranet – Guidance for Local Councillors from the Information Commissioner and the Local Government Association.

3.0 Implications/Consultations

3.1 Information on any corporate issues and consultation associated with this report are detailed in **Essential Reference Paper A.**

Background Papers

CMT 25 September 2012 – Information Security Policy.
CMT 15 May 2012 – Data Protection Update Report.

Contact Member: Councillor Tony Jackson – Leader of the Council, Extn: 1642. 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