EAST HERTS COUNCIL

CORPORATE BUSINESS SCRUTINY COMMITTEE – 12 JULY 2016

REPORT BY HEAD OF LEGAL AND DEMOCRATIC SERVICES

DATA PROTECTION ANNUAL REVIEW

WARD(S) AFFECTED: ALL

Purpose/Summary of Report:

- To update the Committee on the Shared Internal Audit Service (SIAS) Report (**Essential Reference Paper 'B'**).
- To invite the Committee to comment on the current Data Protection status to date.
- To invite the Committee to agree that future scrutiny and monitoring of the council Data Protection risks would be best conducted through Covalent (the councils' performance management system).

RECOMMENDATIONS FOR CORPORATE BUSINESS SCRUTINY: That:	
(A)	**The actions and developments in regard to data protection compliance be noted;**
(B)	**The Executive be advised of any recommendations regarding the Council's data protection compliance; and**
(C)	**The ongoing scrutiny and oversight of data protection compliance via the quarterly healthcheck and use of the Covalent system be agreed.**

1.0 Background

1.1 Corporate Management Team (CMT) adopted an Information Security Framework and priorities for Data Protection (DP) policy development and implementation 25 Sept 2012.

1.2 Governance structures were agreed at Corporate Business Scrutiny (CBS) Committee 19 March 2013, including an annual

update in their governance role (strategic oversight) of the Council's DP 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.

1.4 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. In 2014/2015 this was incorporated into the service planning process, supported by the Digital Media and Information (DMI) team. In 2015/2016 this process was streamlined to allow services to certify compliance for their processes that remained unchanged, allowing them to focus on those areas that had changed and to conduct full compliance reviews on new processes. The streamlined review process was well received.

2.1.2 The DP review within the Service Planning process:

- Enabled services to understand their key DP risks within the context of their developing service.
- Equipped services to embed the management of DP risks into their day to day processes.
- Enabled the DMI team to identify continuing trends in DP risks that would benefit from corporate measures.
- Enabled the DMI team to better support services by creating a formal structure for DP reviews that required a positive action to sign off, rather than a "silence is assumed compliance" approach.

2.2 Corporate Risks

2.2.1 Three corporate risks were identified and reported to CBS in 2014, and continue to be monitored as such:

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

2.2.2 Significant work was undertaken in 2014/2015 to improve understanding of Fair Processing Notices and Data Sharing.

2.2.3 This work has continued, with a review of Fair Processing Notices in use on different forms, and with support for new forms and processes requiring collection of personal data (e.g. Forever Active East Herts project).

2.2.4 Data Sharing agreements have also been reviewed, with both the Housing and Community Safety teams seeking advice and assistance, and the Shared Anti-Fraud Service (SAFS) project relying on a thorough analysis of Data Sharing risks and responsibilities, and drafting of robust agreements and procedures.

2.2.5 Council wide training was undertaken in 2014/2015. This training is due to be refreshed in 2016/2017, but ad-hoc training has also been delivered throughout 2015/2016.

2.2.6 Document Retention and Disposal has been addressed with a number of teams, both those exploring new systems and software, and those looking to reduce storage needs. This is an ongoing area of support for services.

2.3 Key Information Technology (IT) Risks

2.3.1 Previous reviews highlighted four key areas of risk associated with use of IT equipment:

- Increasing use of portable devices by staff and Members.
- Growth in home working.
- Possible conflict between flexibility for users and requirements for high security around sensitive data on the network.

- Use of non-secure email.

2.3.2 Continued developments in the Council IT infrastructure and IT strategy have steadily reduced the risks on the first three of these to manageable levels, with the hosted desktop environment and carefully designed security profiles being key improvements.

2.3.3 The risks surrounding non-secure email remain, but these are considered acceptable, having been addressed in training. The hosted desktop environment has contributed to the reduction in risk, allowing staff to access their work emails within the council network, using the VMware application from any PC, laptop, tablet or smart device.

2.3.4 The Shared IT Service continue to deliver secure and robust technology, with a high level of awareness of the need to accommodate data security at both the strategic level and operational level.

2.4 Policy Development and Training

2.4.1 There is a continued need to ensure that Data Protection and Data Security are included in policy drafting schedules. Both the Shared IT Service, and the HR service are keenly aware of this, and have worked to.

2.4.2 DP continues to form part of the induction programme and has been given a renewed focus, with specific attention given to the training available on the staff intranet, and to the need to take personal responsibility and speak to the DMI team if staff have any concerns at all.

2.4.3 “Bob’s Business”, a training package developed by the Department for Business Innovation and Skills continues to serve as the prime training tool for Data Protection and Data Security awareness. A full rollout of training took place in 2015/2016, which will be refreshed in 2017.

2.5 Member Guidance

2.5.1 DP guidance was issued to Members following the 2015 elections.

2.5.2 Further DP training has been undertaken with Members at HR and Licensing Committees.

2.5.3 There has been ad-hoc advice given to Members on request, and Members are encouraged to contact the data protection officer should they require assistance in such matters.

2.6 Service Based Risks

2.6.1 A number of local risks continue to be identified in the annual Data Protection Risk Assessments.

2.6.2 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 continues to be very good with the number of ad-hoc DP enquiries from staff seeking advice from the data protection Officer increasing.

2.6.3 The corporate restructure, and introduction of new service groupings and new Heads of Service may present challenges from a Data Protection perspective, as processes and procedures may be reviewed and changed, however the previous year's risk assessments should be viewed as tools to be used in shaping any new processes.

2.6.4 Given the directions from senior management observed to date, and the level of shared oversight the new leadership structure has introduced, it is not considered that the restructure presents a significant risk. The consolidated Leadership Team structure, with more frequent meetings than the previous structure, instead offers a more robust platform for ensuring Data Protection compliance, and a more open forum for sharing good practice.

2.6.4 Engagement and commitment from current Heads of Service continues to be excellent, with a number of managers within the services regularly contributing to the risk assessment process. This approach, with Heads of Service asking operational managers to inform the risk reviews illustrates the manner in which services are embedding DP consideration throughout their processes, from the strategic to the operational level.

2.6.5 Some service level risks (particularly those that involve advising customers of their DP rights and the way in which their data will be handled) continue to be addressed through content reviews (e.g. the recent audit of documents/forms on the website).

2.6.6 The council Digital Transformation/Delivery programme is

expected to offer further opportunity to embed robust Data Protection protocols into systems and processes, further reducing Service level risks

2.7 Recorded DP Breaches in 2015/2016

2.7.1 The Council works hard to ensure that all staff quickly identify and address any breach of DP, no matter how small with a focus of ensuring improvements in process and training to continue to reduce the potential for breaches. It is a reality that all organisations have data breaches. It is a huge strength that we recognise and act proactively. The Council does not view any breach as acceptable but it is right to understand that mistakes inevitably occur, and to have in place measures to respond with when they do so.

2.7.2 Three breaches occurred in 2015/2016.

2.7.3 An Email from Revenues and Benefits was sent to the wrong person, when a ".com" suffix in their email address was mistakenly replaced with a ".co.uk" suffix. The majority of the information contained within the email was public, although some matters regarding use of an address and the tenancy of the customer's parents were considered to be personal.

2.7.4 The customer was unhappy with the council's investigation into the matter, and referred the case to the Information Commissioner's Office (ICO) as a complaint. The ICO investigated the case, but found that the council's handling of the matter had been appropriate, and that no further action or recommendations were required. This is considered a validation of the council's Data Protection policies, training, and response to breaches.

2.7.5 A letter was sent to a customer from Revenues and Benefits, which contained a number of pages from a second customer's letter. The information contained some references to bank accounts. On investigation, it was found that the information did not present any significant risk of banking fraud or identity theft. The customer reported the matter directly to the ICO, who conducted an investigation. The ICO found that a minor breach of Data Protection had occurred, but that the council procedures and response to the breach had been appropriate. The ICO did not consider that any further action or advice was required, again, validating the council's policies, training and response.

2.7.6 An email was sent from Housing Advice to a customer, containing details of a risk of homelessness and Social Services referral of a second customer. The information contained a full name, as well as the name and contact telephone number of one of the social workers.

On investigation it became clear that there had been a minor breach of Data Protection, but that the customer details released were not sufficient to allow the receiving customer to identify or locate the subject customer. The release of professional contact details of the social worker was unfortunate in the circumstances, but not a breach of Data Protection given the context of the information.

The customer was extremely unhappy with the incident, but did not pursue the matter with the ICO.

2.7.7 The low number of incidents in 2015/2016, and the ICO's continued satisfaction with the council's responses, as well as our policies and procedures, is testament to the work that the Heads of Services and senior managers have undertaken to ensure that Data Protection awareness is part of the day to operation of their individual teams.

2.8 Other Actions

2.8.1 The Shared Internal Audit Service (SIAS) conducted an Audit of the council Data Protection governance and arrangements. The audit report returned a level of Substantial Assurance, with no improvement recommendations. A copy of the report is attached as ERTP.

2.8.2 The new EU General Data Protection Regulations (GDPR) were consulted on and drafted through 2015/2016. These were adopted in April 2016 and will apply from May 2018. The decision taken at the EU Referendum in June 2016, to leave the EU, means that the council will not be bound by the GDPR, but it remains to be seen if any UK specific legislation will be introduced that replicates the effects of the GDPR. The council has already reviewed current states of compliance against guidance published by the ICO, and expects little difficulty in maintaining compliance with any similar legislation.

The implications of the decision to leave the EU on other Data

Protection frameworks, such as the EU/US Safe Shield framework are yet to be clarified. The council will monitor any risks arising from this and make appropriate recommendations to those services impacted by such frameworks.

2.9 Reporting and Scrutiny

2.10 It is proposed that the ongoing scrutiny and oversight of the council Data Protection compliance be conducted solely through the existing risk management process.

2.11 Current arrangements are that an annual report be made to Corporate Business Scrutiny.

2.12 While an annual report is a useful summary tool, it is a retrospective mechanism, looking back over the entire previous year's performance. The quarterly updates are visible to all Members on Covalent, the council's performance management system, and risk reports to the Executive (via the Healthcheck) and to Audit and Governance Committee, These allow for issues to be identified and addressed much more quickly and are seen as a logical progression in the mainstreaming of Data Protection as a corporate risk issue, reducing the bureaucratic overhead while increasing scrutiny and oversight.

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
None.

Contact Member: Councillor G McAndrew, Executive Member for Environment and the Public Space. graham.mcandrew@eastherts.gov.uk

Contact Officer: Mike Rowan, Head of Legal and Democratic Services, Extn: 2170. mike.rowan@eastherts.gov.uk

Report Author: Mike Rowan, Head of Legal and Democratic Services, Extn: 2170. mike.rowan@eastherts.gov.uk