EAST HERTS COUNCIL

CORPORATE BUSINESS SCRUTINY COMMITTEE – 14 JULY 2015

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 (**Essential Reference Paper'B'**).
- To invite the Committee to comment on progress to date.

RECOMMENDATIONS FOR CORPORATE BUSINESS SCRUTINY: That:	
(A)	**the actions and developments in regard to data protection compliance be noted; and**
(B)	**theExecutive be advised of any recommendations regarding the Council's data protection compliance.**

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.

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 DMIteam to identify continuing trends in DP risks that would benefit from corporate measures.
- Enabled the DMIteam 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:

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

2.2.2 To address the latter two of these, the DMIteam workedat a corporate and service level to improve the understanding at the of data sharing and fair processing notices.

2.2.3 Supported by the Communications team, a number of articles were written and published in ‘Team Update’, the staff magazine, highlighting the key areas for consideration around data sharing and Information Security (IS).

2.2.4 This was accompanied by the introduction of a new training suite called “Bob’s Business”; a set of video tutorials that place DP and ISin the context of a small office environment.

2.2.5 Both the articles and training have been well received, and the DMI have been approached by a number of services to advise and assist in Data Sharing exercises, including;

- Reviewing a request to Housing Services from a Housing Association for details of a number of customers on the Housing register
- Supporting the Revenues and Benefits team in ensuring that the agreements with an external Data Matching provider were DP compliant
- Working to ensure the development of the Shared Anti-Fraud Service was DP compliant from an East Herts perspective and that the DP risks of that project were clearly identified and managed in a robust and transparent manner.

2.2.6 We can be confident that most services are compliant withfair processing notices, but ongoing support is needed for a small number of areas wherethey collect data, to ensure that their customers are fully aware of the way their information handled.

2.2.7 Addressing the issues of document retention and disposal has proven to be more problematic, with issues identified around IT systems and databases, the process behind off-site archiving and storage, and the large amount of paperwork that is held across a number of storage sites. Practical steps to mitigate these risks are in place.

2.3 Key Information Technology (IT)Risks

2.3.1 Reviews have 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 The IT strategy delivered by the Head of Business and Technology Services has addressed the first two risks through the deployment of a hosted desktop solution, whereby the user device is insulated from the corporate network. This is supported by remote printing to the council offices and the continued application of policy and training by services reliant on home workers.

2.3.3 Possible conflict between flexibility for users and requirements for high security around sensitive personal data on the network have been addressed with the inclusion of segregated area (known as an Impact Level 3 "bubble") in the network. This allows more stringent security measures to be placed on those users accessing that data which has been assessed as high risk and allows the security policies in operation to be tailored to fit user needs and information security standards.

2.3.4 The risks surrounding non-secure email remains a concern, but has been addressed through training. Appropriate software and technical measures are in place to allow compliance, but it remains for staff to commit to using the systems, and where managers identify an issue, for them to seek training and support to address this.

2.3.4 The new IT Strategy provides a flexible approach to risk within the framework that addresses individual service needs, and a robust assurance of DP and IS within an environment that is sensitive to the context the data is held in. This continuing approach has been validated through the receipt of a substantial level of assurance from a recent audit of IT.

2.4 Policy Development and Training

2.4.1 The Council's revised staff policy "Policy for Handling Data Protection" was approved by CMT on 24/04/2015, and is scheduled to be tabled before Local Joint Panel on 17/06/2015 and Human Resources Committee on 08/07/2015.

2.4.2 IT policy development is led by Shared IT Services.The 4 relevant policies are in draft and expected to be complete by the end of

June 2015 for review by the IT Security Group, for consultation. The policies are:

- Bring Your Own Device (BYOD), addressing the use by staff of their personal mobile devices i.e. smartphones and tablets.
- General IT Security
- Security of Mobile/Portable Data i.e. laptops, tablets, smartphones etc.
- Email and Internet Acceptable Use

2.4.3 The new Staff Handbook has been drafted to include a revised section on DP.

2.4.4 DP forms 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.

2.4.5 During the 2013/2014 DP review process, a number of services identified the need for more contextual training; that is, training that contained specific examples of day to day work, rather than higher level training that addressed legislation and general principles.

2.4.6 “Bob’s Business”, a training package developed by the Department for Business Innovation and Skills was identified and agreed as a suitable product, and training with this has been ongoing since December 2014. This is a module based system, with a new module being released every month. This is used in conjunction with the more general training on principles and legislation that remains available on the staff intranet. It is recommended that “Bob’s Business” continue for new staff, with the more general training being kept to act as a resource for all staff.

2.5 Member Guidance

2.5.1 DP guidance was issued to Members following the 2015 elections. So far, 23 Members have confirmed receipt and understanding. This will continue to be issued annually, with Members requested to confirm their receipt and understanding.

2.5.2 Further DP training has been undertaken with members at the Member Induction day and CBS.Further training for HR and Licensing committees is scheduled.

2.5.3 DP guidance is available on the Members Extranet, currently under the New Member Induction section. A project to review the Members Extranet is underway (assisted by Socitm, the public sector IT professional body). Provision of DP guidance will be part of the recommendations of that project including committee specific guidance.

2.5.4 Further specific guidance will be developed to support services engaging with members, e.g. Social Media and DP Implications - developed to support the Communications team.

2.6 Service Based Risks

2.6.1 A number of local risks were identified during the review process, some unique to just one service. These are summarised in the action plan (ERP B). Services will be re-visited by the IDM team to check progress against their recommended actions.

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 increasing.

2.6.3 Heads of Services re-certified their compliance and risksthis year rather than having to repeat a full DP review where no changes had taken place to their processes. This is the first year that the re-certification process was included within the Service Planning process. This has been considered to be a sensible and productive development beyond the full review process.

2.6.4 Engagement and commitment from Heads of Service has been excellent, with a number of managers within the services contributing to the 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) will be addressed through a service level digital content development project, addressing all aspects of web content.

2.7 **Recorded DP Breaches in 2014/2015**

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 An Email from Development Management to a number of consultees left each consultee's email address visible to all recipients. Most email addresses were either already public or professional use. Minor breach, not reportable to the Information Commissioners Office (ICO).ICO guidance states this kind of matter should not be reported to them. The error was immediately recognised and addressed by the relevant manager.

2.7.3 Document emailed in error to Council tax customer, containing bank account details of other customers. The information was recovered, remedial steps were taken. Reported to ICO. The ICO agreed that the council had sufficient measures and training in place to satisfy their requirements, and that the council had responded appropriately to the breach. The ICO did not undertake any sanctions against the Council nor require any further action from the Council.

2.7.4 An email was sent to an external HR advisor in error, containing details for an occupational health referral. The advisor is Director of the regional LGA HR team, and has been involved in a number of sensitive HR issues, acting to give advice and support. This was considered a technical breach that did not require reporting to the ICO. The ongoing relationship between the council and the LGA HR Director, and their professional position and knowledge meant the matter did not present any significant risk.

2.7.5 2 minor breaches where Council Tax letters were sent to incorrect addresses. These occurred where accounts had been held jointly due to shared occupancy, and where the shared occupancy had ceased (partners separated or house/flat mates moved on) but account details remained connected on the database. In both cases the parties involved were advised, and steps taken to

disassociate the accounts. The Head of Revenues and Benefits took immediate steps to ensure that address updates were scrutinised for associations with other accounts and that as matter of course this process would be monitored more thoroughly.

2.7.6 The response from the ICO in the matter of the release of bank account details (a serious breach of Data Protection that might have been expected to give rise to a financial penalty) is a validation and endorsement of the Council's approach to DP, and the processes we have in place to mitigate risk and respond to breaches. While we must not be complacent, nor consider such breaches to be acceptable, we are right to understand that mistakes inevitably occur, and to have in place measures to respond with when they do so.

2.8 Other Actions

2.8.1 The Audit of Data Protection by Shared Internal Audit Service (SIAS), planned for late 2015/2016 was brought forward when SIAS were able to identify an opportunity created by other audit schedules being re-arranged. We await their report and recommendations.

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: CouncillorGraham McAndrew – Executive Member for Environment and the Public Space.
graham.mcandrew@eastherts.gov.uk

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

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