Report author: Louise Whitworth, Paul Burns and Julie Davison

Tel: 07891 276168

Report of Director of Resources and Housing

Report to Corporate Governance and Audit Committee

Date: 22 January 2018

Subject: Information Management and Governance – Update on Public Services Network (PSN) Submission and Cyber Position and the Implementation of the new Data Protection Framework (GDPR)

Are specific electoral Wards affected? If relevant, name(s) of Ward(s):	☐ Yes	☒ No
Are there implications for equality and diversity and cohesion and integration?	☒ Yes	☐ No
Is the decision eligible for Call-In?	☐ Yes	☒ No
Does the report contain confidential or exempt information? If relevant, Access to Information Procedure Rule number: Appendix number:	☐ Yes	☒ No

Summary of main issues

1. The Public Services Network (PSN) was set up as an assured route for information sharing by central Government, to facilitate shared services and also serve as the assured route for Government Connects Secure Extranet (GCSx) mail. It acts as a compliance regime that serves as both a commitment to a basic level of information security for connecting government departments and local authorities and also a level of trust between Leeds City Council and other public services.

2. Due to more stringent compliance controls brought in by the Cabinet Office in 2014 the Council are presently unable to meet the PSN certification requirements. The Cabinet Office contacted the Council through the Chief Executive in January 2017, to ensure that the Council brings itself into compliance as soon as possible. The Council's access to the PSN has not been unduly restricted but this would be a likely consequence if prompt action was not taken.

3. The EU General Data Protection Regulation ("the GDPR") was adopted in May 2016 and will be directly applicable in all EU member states from 25 May 2018. The new Data Protection Bill, announced in the Queen's Speech, will bring new EU law (the GDPR and the Data Protection Law Enforcement Directive) into

domestic law; exercise the available derogations in the GDPR; and repeal the Data Protection Act 1998.

4. There are only 5 months left before the GDPR takes effect and the law will impact on how personal data and sensitive personal data is processed throughout its life cycle across every service in every directorate. It will impact on every officer within the Council and will also impact on those contracts with suppliers where personal data is processed and the Council's relationships with partners and stakeholders.

Recommendations

Corporate Governance and Audit Committee is asked to consider the contents of this report and be assured of the council's approach to Information Governance and specifically in this case PSN compliance and the implementation of the changes required to achieve compliance with the new legislation from May 2018.

1. Purpose of this report

To provide Corporate Governance and Audit Committee with an update on the current position on Cyber Assurance and Compliance, specifically compliance to the PSN Assurance standard and with an update on the council's plans for implementation of GDPR.

Update on Public Services Network (PSN) Submission and Cyber Position

2. Background Information

2.1 The Public Services Network (PSN) was set up as an assured route for information sharing by central Government, to facilitate shared services and also serve as the assured route for (secure) GCSx mail. It acts as a compliance regime that serves as both a commitment to a basic level of information security for connecting authorities and also a level of trust between Leeds City Council and other public service.

2.2 Due to more stringent compliance control brought in by the Cabinet Office in 2014 the council are presently unable to meet the PSN certification requirements. The Cabinet Office has placed the council into an 'escalation' process for PSN, a process by which the Cabinet Office seek commitment from the CEO and provide further support in remediation against the controls.

3. Main Issues

3.1 In February 2017, the Council received the IT Health Check (ITHC) results for 2017; an annual audit required for PSN compliance. The ITHC report for 2017 detailed vulnerabilities across the infrastructure. This audit followed the cabinet office' scope requirements for PSN and as such the number of issues the council had to address had grown significantly from 2016.

3.2 A significant number of individual vulnerabilities were revealed on a 10% sample of the estate. The sheer size and volume of unknown issues across the estate gave evidence to systemic failure of controls, previously believed to be sufficient.

3.3 The PSN Assurance Team (Cabinet Office) mandates that each vulnerability is extrapolated to the estate as a whole and resolved. Those identified as critical or high must be resolved before the Local Authority can be determined compliant.

4. Actions to Date

4.1 The PSN Remediation Board, with the Head of Information Management and Governance as Senior Responsible Officer (SRO), reporting to CLT and the Senior Information Risk Officer (SIRO) monthly, has made significant progress. The board meets bi-weekly to work through the compliance requirements and close down remediation tasks realised by the ITHC audit. Monthly meetings with the PSN Authority (PSNA) provide them with regular reports about the progress being made by the council. This relationship is strong and supportive.

4.2 Network Attached Devices – The ITHC in February 2017 highlighted a large number of issues on a sample of the network. This was due to process defects with patching and configuration management. The estate is now being actively monitored for vulnerabilities and patched appropriately. Compliancy is now above 90% for Windows hosts (which comprises of the bulk of the estate) and which is an acceptable level for the Regulators. 146 unsupported or un-patchable Windows servers have been removed from the estate,

4.3 Housing BI Reporting – The User Acceptance Testing due in November 2017 was delayed due to the complicated nature and inter-relationship of the databases involved. The issues have now been, however the delay has meant that completion of this workstream will be pushed to the end of January 2018.

4.4 Telephony – All Polycom devices have been updated and a process has been established to ensure they are kept up to date in the future.

4.5 Solaris / Siebel - All out of support Solaris servers and all occurrences of out of support Siebel have either been removed from the estate or ungraded appropriately.

4.6 Applications – 32 Cloud suppliers have been identified. They have all been contacted regarding their compliance with the 14 PSN Cloud Security Principles. To date, 29 have been returned. Cloud Principles have been added into technical specifications for all new contracts and renewals. In development is a ‘Cloud Readiness Assessment’ for external suppliers to ensure that they meet the Principles prior to tender.

4.7 Mobile Device Management – A pilot has been carried out with Digital Information Service staff. The support documentation has been amended in light of feedback received. A temporary pause in the full rollout has been called to ensure all issues are addressed, but a roll out to a further cross section of 50 users is taking place in January 2018.

4.8 Network Segmentation / Authentication – The procurement of a network access control software is complete, implementation is planned before the end of March 2018. Network segmentation will follow the completion of this work.

4.9 A re-application for PSN Certification was made to the Cabinet Office on the 30th September 2017. In November 2017, a mid-year IT Health Check was instigated in order to ratify the Council's position. The results of the ITHC show a significant improvement. Where vulnerabilities were highlighted, there was nothing that we were not already aware of and plans were already in place to rectify. The Cabinet Office asked for a copy of the November ITCH report to compare with our September PSN submission. To date we have had no response from the Cabinet Office regarding our PSN status, although verbal conversations have been very positive, with recognition of the considerable effort and large amount of work completed so far.

Implementation of the new Data Protection Framework (GDPR)

5. Background information

5.1 The GDPR is the most significant development to data protection law since the Data Protection Act 1998 (DPA). The GDPR, and the Data Protection Bill that is currently going through parliament, are designed to bring about more fairness, transparency and security into the way we hold data.

5.2 While the GDPR is building on the principles already in place under the DPA, the GDPR's emphasis elevates their significance and places greater accountability on organisations to demonstrate their compliance with the new legislation.

6. Main issues

6.1 A project of this size is a significant programme of work and dedicated resource is required to make the relevant people, process and technology changes required across the council to enable us to be compliant by May 2018 and maintain that compliance thereafter.

6.2 The council has a number of highly experienced IM&G practitioners who are both leading on and involved in each of the work streams. However, work on GDPR in the most part is an 'add on' to business as usual including work on statutory requests, high risk matters, and projects to deliver strategic and directorate led objectives.

6.3 To address this a GDPR Implementation Team was established in August 2017 for a fixed term of 12 months.[1] This team is led by the Corporate IM&G lead for Access and Compliance. This team consists of:

- 2 x Senior Information Governance Officers from within the IM&G Service;
- part time support from a project manager and a project support officer within PPPU

The role of this team is primarily to:

- project manage and coordinate all the activities, outputs, and interdependencies of the work streams;
- develop a framework / package to empower the business to adopt and accept responsibility for implementing GDPR;
- roll out of the framework / package across the council via GDPR Service Leads;
- support services with the work required to implement GDPR by being the first point of contact for all matters relating to GDPR; and
- ensure that the governance and reporting arrangements for a project of this size are adhered to.

6.4 The GDPR implementation team requires active engagement and support from core services within the council such as ICT, Legal, HR, Procurement, Communications and Internal Audit.

7. Actions to date

7.1 Data Protection Officer - The GDPR requires the council, as a public authority, to designate a Data Protection Officer ("a DPO"). The main tasks of the DPO are: to inform and advise the council of its obligations under GDPR when processing personal data; to monitor compliance with the GDPR; to provide advice where requested, particularly, with regards to Data Protection Impact Assessments and other high risk processing activities; and to act as the contact point with the supervisory authority (the ICO). A DPO may be designated for several public authorities and bodies but must be supported in performing his/her tasks through the provision of the necessary resources. Furthermore, the GDPR establishes some basic guarantees to help ensure that DPOs are able to perform their tasks with a sufficient degree of autonomy within their organisation.

7.2 The Council's Head of Information Management and Governance (Louise Whitworth) has been appointed as DPO. This decision was ratified by the Information Management Board on 9th August 2017, the appointment being made with immediate effect.

7.3 Technical workstreams - Since September 2016 much work has taken place to assess the requirements of the GDPR and the Council's current position against the requirements. From this initial assessment 9 technical workstreams were

[1] Whilst there is no dedicated funding for GDPR, this team is to be funded from within Resources and Housing's budget.

initiated to define the objectives and outputs required to achieve compliance with the relevant articles in the GDPR and to ensure that appropriate policies, procedures and guidance are updated or created.

7.4 The 9 technical workstreams are as follows:

- Demonstrating compliance
- Security of processing
- Security incident management
- Data Protection by design and default
- Contracts with data controllers / processors
- Individuals' rights
- Lawfulness, fairness and transparency
- Storage limitation
- Accuracy and data quality

7.5 GDPR Implementation Events - Throughout the month of November 2017, the GDPR Implementation team has delivered a series of 2 hour engagement sessions to which all senior management across the authority received invitations. The purpose of the events were to give directors, chief officers and heads of service an overview of GDPR, what the key changes are, and what their responsibilities are for implementation. In total 188 officers attended, including 158 senior managers across all services, and 30 HR and DIS Business Partners.

7.6 GDPR Service Leads - These roles will be critical to the implementation programme and the key responsibilities of these GDPR Service Leads are to:

- support the GDPR implementation team by driving the GDPR agenda within service areas including the dissemination of key messages;
- ensure that existing processing arrangements and systems are GDPR compliant and, where required, make the necessary changes including the implementation of appropriate technical and organisational measures proportionate to the risks involved;
- assist with the embedding of new GDPR related policies and procedures across the council;
- report progress on implementation against key milestones to the GDPR implementation team including the reporting of risks and issues as they emerge; and
- support the IM&G Service with post 'go-live' monitoring and compliance audits.

7.7 Following discussions at the GDPR Strategic Implementation Board (SIB), Information Management Board and CLT, Chief Officers have been tasked with identifying a minimum of one GDPR service lead for the service areas under their responsibility.

8. Consultation and Engagement

8.1 Consultation on the development of strategies, policies, procedures and standards are extensively undertaken across a broad range of stakeholders including information management professionals, representatives from all directorates via representatives of Information Management and Technology Teams and Information Management Board members.

8.2 A report is has been presented to the CJCC on the Council's implementation plans for GDPR and further engagement will be discussed at the next meeting.

8.3 A briefing note is currently being prepared regarding GDPR for members and further talks are scheduled for early 2018 to scope the requirements of members which could include briefing sessions and training packages.

8.4 A Cyber Training session for members took place on the 12th January 2018.

9. Equality and Diversity / Cohesion and Integration

9.1 Equalities, diversity, cohesion and integration are all being considered as part of delivering the Information Management and Governance Strategy. This refers to the way training is being delivered as well as how policies will impact on staff and partners.

9.2 The GDPR implementation team are currently in discussion with HR regarding the format and delivery of a GDPR themed appraisal objective for all staff cascaded via Directors.

9.3 The GDPR implementation team will be engaging with the council's staff networks with a view of obtaining their input into the design of material, eg posters, one minute guides etc.

9.4 The third version of the mandatory managing information training level 1 will be rolled out to all staff in early 2018 which has been updated to include the changes under GDPR and an increase emphasis on Cyber.

10. Council policies and City Priorities

10.1 All information governance related policies are currently being reviewed and a dedicated Policy Review group has been established. As part of this review the group will be consulting with internal stakeholders and external peer checking.

11. Legal Implications, Access to Information and Call In

11.1 Delegated authority sits with the Director of Resources and Housing and Senior Information Risk Owner and has been sub-delegated to the Chief Information Officer under the heading "Knowledge and information management" in the Director of Resources and Housing Sub-Delegation Scheme.

11.2 There are no restrictions on access to information contained in this report.

12. Risk Management

12.1 Should action against the current PSN Remediation plan not be to the satisfaction of the PSN Authority, the Council will have to withstand a number of risks:

- The Head of the PSN has informed the Department of Works and Pensions of our non-compliance. Continued non-compliance could culminate in the switching off of GCSx mail and access to Revenues and Benefits data.
- The Head of PSN will inform the Information Commissioners Officer, which could culminate in the revisiting of the audit conducted by the ICO in 2013 to ensure compliance against the Data Protection Act.
- The Head of PSN will inform the Deputy National Security advisor to the Prime Minister, who would in turn conduct an assessment based on the national risk profile.
- The Head of PSN could instigate an external audit of all our security systems by the National Cyber Security Centre. The Council could end up under partial commissioner control.
- Ultimately, the Head of PSN could instigate a complete 'switch off' from PSN services

12.2 PSN certification is relied upon as an assurance mechanism to support information sharing, where many of the requirements request that the council present a certificate prior to sharing, or evidence alternative, more time consuming, compliance work to be completed. This has had an impact already on sharing with Health as a number of the controls required for the NHS Information Governance Toolkit are evidenced by a PSN certificate.

12.3 Without a PSN certificate, there is significant risk to the council's National reputation as a Digital Innovator.

12.4 The risk associated with not implementing GDPR compliant information governance policies, procedures and practice across the council leaves the organisation more susceptible to breaches of legislative, regulatory and contractual obligations, affecting the confidence of its citizens, partners, contractors and third parties when handling and storing information.

12.5 Information risk is being systematically addressed by joining up the approach to risk required by information security standards, the need for the senior information risk owner to be clear about the risks he/she is accountable for and the council's standard approach to risk management.

12.6 Further work is being undertaken in conjunction with the Corporate Risk Manager to embed the recording and reporting of information risk monitoring and management relevant to this project. The Information Asset Register project will generate information required and an automated dashboard will be produced to report risk assessments to the SIRO. This will provide the assurance required by the SIRO from the business and will allow risk mitigations to be prioritised.

13. Conclusions

13.1 The establishment of improved Information Management and Governance in the Council's technical infrastructure and improved practice and procedures outlined in this report (with regards to Cyber and GDPR) provides a level of assurance to Committee that the range of information risk is being managed both in its scope and through to service delivery. It allows the council to work with partner organisations, third parties and citizens in a clear, transparent, but safe and secure way. It helps to protect the council from enforcement action and mitigate the impact of cyber incidents and other Data Protection breaches.

14. Recommendation

14.1 Corporate Governance and Audit Committee is asked to consider the contents of this report and be assured that considerable effort is being undertaken to rectify the current situation with regards to the Council's approach to information governance and specifically in the case of PSN compliance where significant progress has been made.

14.2 Corporate Governance and Audit Committee is asked to consider the contents of this report and be assured of the council's approach to implementation of the changes required to achieve compliance with the new Data Protection legislation from May 2018.