OXFORDSHIRE COUNTY COUNCIL

Audit & Governance Committee
Wednesday, 11 September 2019

ADDENDA

8. Information Governance (Pages 1 - 6)

3.10pm

Report from the Director for Law and Governance (Attached.)

The report highlights the work of the Information Management team to give assurance on how these issues are handled within the Council.

The Committee is RECOMMENDED to note the report.

This page is intentionally left blank

Division(s): N/A

AUDIT AND GOVERNANCE COMMITTEE – 11 September 2019

Information Management Report (Sep 2018 to Aug 2019)

Report by Director of Law & Governance and Monitoring Officer

RECOMMENDATION

1. The Committee is RECOMMENDED to note the report.

Purpose of the Report

2. To provide assurance to members of the Audit & Governance Committee as to the approach taken to Information Management within the Council

3. This report includes the actions undertaken by the Information Management team to ensure Oxfordshire County Council is compliant with the DPA 2018/GDPR.

4. Information Management and the protection of personal data should clearly be an integral part of the business of the Council. The protection of personal information is every officer's responsibility and the Information Management team coordinates both the policy agenda for this work within the Council together with appropriate practical interventions to manage our statutory duties.

5. This report summarises some of the work of the Information Management team over the previous year.

Governance

6. There are two boards that provide governance of information management within the council: The Information Governance Group and the Information Governance Board.

Information Governance Group

7. The objective of the Information Governance Group is to inform, coordinate and direct the work of others as appropriate to ensure that there is a co-ordinated approach to Information Governance compliance across the council and with our partner organisations, and to provide assurance to the Information Governance Board on the effectiveness of the information governance arrangements within the council.

8. The group is chaired by the Information Services Manager. Group membership is the Information Services Manager (Deputy Data Protection

Officer), Deputy Senior Information Risk Owner, Deputy Caldicott Guardian, Service Information Governance Leads from Adult Social Care and Children, Education and Families and representatives from Cultural Services, ICT, HR and Customer Services.

9. The Information Governance Group reports into the Information Governance Board.

Information Governance Board

10. The objective of the Information Governance Board is to provide leadership and guidance on information governance matters across the council and with our partner organisations, and to provide challenge to the Information Governance Group.

11. The group is chaired by the Director of Law & Governance (Data Protection Officer). Group membership is the Data Protection Officer, Senior Information Risk Owner, Caldicott Guardian, Information Services Manager (Deputy Data Protection Officer), Deputy Senior Information Risk Owner and Deputy Caldicott Guardian.

12. Each group meets on a monthly basis.

DPA/GDPR Compliance

Data Protection Impact Assessment/Information Management Risk Assessments

13. All new systems and processes require a Data Protection Impact Assessment; this will assess for compliance with DPA/GDPR and also identify any areas of concern regarding information security. Those with additional information security requirements or concerns will have additional checks in the form of an Information Management Risk Assessment.

14. The team has received or identified the need for 112 new Data Protection Impact Assessments or Information Management Risk Assessments during this period.

Individual Rights Requests

15. The team has received 265 individual rights requests. The majority, 253, were subject access requests (SAR's). The other were requests for change inaccurate personal information (2) and deletion of information (10).

Information Asset Register

16. The annual review of the Information Asset Register (IAR) has begun. The IAR is important as it identifies the information we hold, and how we manage, process and share that information. Having an accurate, up to date IAR is a key factor in ensuring we are compliant. The IAR also provides a register of the information held by the organisation which can be used by individual teams, projects and business intelligence. The review consists of approx. 50 separate staff interviews and is not expected to be complete until the end of December 2019.

17. Once each register is complete it is analysed to identify areas of concern e.g. no sharing agreement, no consent etc. and marked for action. Once this is done an assessment will be made of the security and legality of processing; and changes to processing requested as needed.

Information Sharing Agreements

18. Information Sharing Agreements (ISA's) are required to ensure we are sharing information securely and within the requirements of DPA/GDPR. If there is a contract in place the sharing agreement is included in the contract. If there isn't a contract, e.g. if sharing information with a partner organisation, an Information Sharing Agreement is required. The team do not write the sharing agreements but do check they are in place and fit for purpose.

19. The organisation has multiple ISA's but these are not published within OCC, this can result in multiple ISA's with an organisation (e.g. with the NHS). The team are reviewing and collating the ISA's identified during the Information Asset Register interviews to streamline and remove redundant ISA's. Once complete they will be published on the intranet.

e-learning

20. All staff, councillors and contractors need to complete the mandatory Acceptable Use and Data Protection Essentials e-learning courses on an annual basis. The Data Protection Essentials course has been reviewed and updated; the launch of the annual completion for all staff is planned for 30th September.

Awareness

21. Awareness of information governance has continued throughout the year with monthly intranet headlines and regular yammer posts. In addition, the main section of the August Manager's Briefing was dedicated to information security.

Information Management Policies

22. There is a suite of information management policies that are designed to ensure effective governance of the information we hold:
    - Acceptable Use Policy
    - Access to Information - Security Vetting Policy
    - Data Protection Policy
    - Data Sharing Policy
    - Disposal of ICT equipment policy
    - e-mail Policy
    - ICT Access Policy
    - ICT Software Policy
    - Information Access and Protection Policy
    - Information Security Incident Policy
    - Infrastructure Security Policy
    - Records Management Policy
    - Remote Working Policy

- Removable Media Policy
- Security Classifications Policy

23. All policies are reviewed and updated on a rolling basis over a period of 12 months; all of the above policies have been updated during the reporting period.

Projects

24. The main project the team have been supporting is the implementation of Liquidlogic Children's System (LCS), the new children's social care system. This included agreeing the data migration sign off criteria and signing off over the go-live weekends, completing all the IMRA's, defining and agreeing the data retention periods, clarifying the consent requirements for placement and medical treatment, reviewing and agreeing forms, defining and agreeing system access controls and supporting end to end testing.

25. The team have also been involved with the Digital Platform; this has mainly consisted of Information Management Risk Assessments and ensuring compliance with DPA/GDPR.

26. The team will be engaging with Transformation in a similar manner to other projects, but with the addition of ensuring Privacy By Design is built in where relevant.

Information and Advice

27. In addition to all of the above, the team have dealt with just over 500 requests for information or advice.

Joint Working

28. The team have been providing an information management service to Cherwell District Council since June 2019. This has had an equivalent impact of 0.5 FTE on the team. This impact will continue to be monitored over the next few months

Income Generation

29. The team successfully bid against external organisations to perform a Data Protection Health Check for OxLEP. The review took place at the end of April with follow up meetings taking place in June. The team will be providing a data protection service to OXLEP, the extent of the service is still to be decided.

Potential Security Incidents

30. All potential information security incidents are reported to the team. These are assessed for the seriousness of the breach, risk and impact. The majority of the reported incidents relate to personal information disclosed to an incorrect recipient, lost or stolen, or sent insecurely. The Information Management team

continue to work with the teams involved to review and improve their processes and raise awareness with staff. The team also investigate how we can use the technology available to prevent future incidents.

31. The highest number of potential incidents are reported by the People directorate, this is as expected due to this directorate collecting, storing and sharing most of the personal and sensitive information processed by the council. For this reason, they are also potentially more conscientious about reporting potential security incidents.

32. During the reporting period, 6 incidents were reported to the Information Commissioner's Office (ICO). All were closed by the ICO with no further action by them, but with suggested actions for OCC to mitigate further incidents

Accreditations

33. The team has applied for the annual re-accreditation of the Data Security and Protection Toolkit (DSPT). The DSPT accreditation is needed to access and share information with the NHS. It is a self- assessment against a series of requirements, mainly of processes, procedures and policies. The criteria changed this year and has highlighted a number of areas where the organisation will need to improve/change its processes; the need for improvement/changes will not prevent the accreditation being awarded. The team will be working on these over the next few months.

34. The re-accreditation for Public Services Network (PSN) was also successfully applied for. This is needed for accessing government information e.g. DWP. An independent assessment of the network and building security is done by external security consultants which identifies potential vulnerabilities. The team worked with ICT to address these vulnerabilities.

NICK GRAHAM
Director of Law & Governance and Monitoring Officer

This page is intentionally left blank