Report to Audit Committee

Data Protection Update

Portfolio Holder: Councillor Abdul Jabbar MBE – Deputy Leader and Cabinet Member Finance and Corporate Services

Officer Contact: Anne Ryans – Director of Finance

Report Author: Barbara Mulvihill – Data Protection Officer

4 June 2020

Purpose of Report

To update Members of the Audit Committee on the Council's management and assurance in relation to data protection.

Recommendations to the Audit Committee

The Audit Committee is asked to consider and note the contents of the report.

Audit Committee 4 June 2020

Data Protection update

1 **Background**

1.1 The Audit Committee, as the appropriate Committee within the Council has received a previous Data Protection Officer (DPO) report and agreed to receive reports twice yearly there-after. This is the second update report for 2019/20 (postponed from the 26 March 2020 Audit Committee meeting which was cancelled due to the national COVID-19 lockdown).

2 **Current Position**

2.1 The Council DPO continues to provide advice and guidance to the Council and through formally agreed service level agreements (SLA) to Unity Partnership Ltd (UPL), MioCare CIC and 57 schools (directly maintained and academies) based in Oldham.

2.2 Under the same SLAs, the Information Management Team continues to provide support and expertise across the wider information governance arena, e.g., data protection, information security, Freedom of Information, records management, for these organisations.

2.3 The Information Management Team has commenced delivery of an Information Governance Plus model SLA with Children's Services to drive the implementation of information governance on a variety of services/projects including Oldham Family Connect, Early Help, MASH and the Oldham Partnership.

2.4 The Data Protection Board continues to meet every two months to receive data protection plan progress updates and to discuss information management requirements in relation to local and wider Greater Manchester Combined Authority (GMCA) activities.

2.5 As a consequence of the increased number of localised and GMCA activities/initiatives that require the use of personal information, there is a requirement to ensure that data protection implications are fully considered.

2.6 Examples of the working together of organisations, e.g., Councils, NHS, police, voluntary organisations, housing providers, community groups etc. include, but are not limited to:

- Co-location and integration of services
- Sharing of personal data
- Joining up individual's records
- Development of IT systems to facilitate the above
- Communicating to individuals about the use of their personal data
- Handling of information rights requests within integrated services.

2.7 These activities can be illustrated below:

2.7.1 Oldham Cares has an integrated approach to 'systems of care' in relation to health and social care services. The key aims include, but are not limited to:

- Improving health outcomes and performance
- Focusing on prevention and for people to live healthy lives
- Enabling people to make informed choices
- Working jointly with partners and being needs led
- Developing community resilience through the Thriving Communities project

- A key element of Oldham Cares surrounds the implementation of the Integrated Care Record and the wider Local Health and Care Record Exemplar (LHCRE) programme.

2.7.2 Place Based Integration and Reform focusses on how mainstream services should be delivered across the whole system and in partnership with residents. This will be achieved through the implementation of the Our Oldham Place Based Operating Model. The model aims to create integrated services working in an asset-based way to delivery better outcomes for people and the places where they live. These changes in delivery will work in partnership with the Thriving Communities project which is part of Oldham Cares.

2.7.3 This area of work feeds into the GM Place and Reform Executive and towards the implementation of the Place Based Reform Greater Manchester Model.

2.8 The Council's Information Management Team is working closely with colleagues from other organisations to ensure that information governance requirements are considered and built into initiatives as they are developed. There is a particular focus currently on ensuring that data protection requirements continue to be met, whilst ensuring data sharing supports the COVID-19 efforts.

2.9 The DPO will be working alongside the Information Management Team and other services to further develop a wider assurance role in order to evidence compliance and best practice in relation to the handling of personal data and compliance with data protection.

2.10 The submission for the Council's PSN (Public Services Network) annual mandatory accreditation was submitted and agreed as meeting the standard for the period ending 31 March 2020. The submission demonstrates how the Council's security controls are sufficiently rigorous to use the PSN network to collaborate and share information with other public services.

2.11 The submission of the Council's Data Security and Protection (DSP) annual mandatory accreditation is usually made before the end of March, however, as a result of the coronavirus deadlines have been extended to September 2020. This submission demonstrates how the Council's information management controls, (with a focus on Adult Health and Social Care), meet the standards set out in the toolkit. It is a requirement of the Department of Health that all organisations who handle adult health and social care personal data complete the toolkit.

2.12 Changes within the Data Protection Act 2018 had a significant impact on how requests for information should be handled by the Council. The Information Management Team is implementing the Data Protection Compliance Improvement Project, that aims to ensure systems and processes are suitable to support the implementation of these changes. The project is currently focussing on the process for managing subject access requests. Phase 1 of this work has now concluded, with the current process analysed and feedback gained from all stakeholders on how the processes and overall performance could be improved. Phase 2 is focusing initially on identifying a route for a new IT solution before moving onto implementation.

2.13 There have been security incidents during 2019/20 and these have been and continue to be actively managed by the Information Security Manager. A summary by Directorate is attached at Appendix 1. There were no serious incidents which resulted in the network losing its capability for a sustained period of time.

2.14   Cybercriminals continue to be a threat and are preying on fears of the coronavirus by sending 'phishing' emails with the aim of getting users to click on a malicious link. It is important to remember that a single malicious link could lead to a successful attack, which could in turn compromise our IT network and put our information at risk. Communications have been sent to all employees and Councillors requesting completion of the Council's interactive Cyber Security training course, available through the MeLearning e-learning platform.

2.15   The Council's Central Records service is relocating from its current site at Vulcan Street to a new location at the Meridian Centre with the key parties managing this move being the Information Management Team, UPL and the Council's Regeneration team. The planned re-location was anticipated to be completed by end April 2020, with the majority of the records transferred to the new site, however, this is currently delayed because of the coronavirus. A visit is to be arranged for Dr Carolyn Wilkins, Chief Executive and Accountable Officer and Cllr Jabbar, Deputy Leader and Cabinet Member Finance and Corporate Services.

2.16   Support is provided to the Council, Miocare, UPL and schools in the delivery of their data protection responsibilities. Previous focus has been on providing tools and advice in the following areas:

- Training and awareness
- Assurance Framework
- Data Protection Policies
- Privacy Notices
- Records of Processing Activities (ROPA)
- Information Governance Logging Systems Development
- Delivery of Continuing Support to Key Partners

2.17   It is envisaged going forward that the focus of the plans will be to build on existing 'business as usual' by continuing to support the Council, Miocare, UPL and schools in their day to day application of data protection and best information practice. The focus of the next phase of the plan will be on bringing to conclusion any residual items in progress at the time of writing and develop a stronger framework around assurance.

2.18   The UK has now entered a 12-month transitional period in relation to leaving the European Union and in terms of data protection there are no changes. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/statement-on-data-protection-and-brexit-implementation-what-you-need-to-do/

3   **Options/Alternatives**

3.1   The options presented for consideration are:

Option 1 - The Committee considers and notes the contents of this report.
Option 2 - The Committee considers the report but requests further information

4   **Preferred Option**

4.1   The preferred option is Option 1 - The Committee considers and notes the contents of this report.

5   **Consultation**

5.1   Relevant officers of the Council have been consulted in the preparation of this report.

6　　　**Financial Implications**

6.1　　N/A

7　　　**Legal Services Comments**

7.1　　N/A

8　　　**Co-operative Agenda**

8.1　　Committed to the Borough - to visibly demonstrate that the Council is taking steps to ensure legal compliance.

9　　　**Human Resources Comments**

9.1　　N/A

10　　**Risk Assessments**

10.1　It is good practice for those charged with governance to consider matters relating to data protection.

11　　**IT Implications**

11.1　N/A

12　　**Property Implications**

12.1　N/A

13　　**Procurement Implications**

13.1　N/A

14　　**Environmental and Health & Safety Implications**

14.1　N/A

15　　**Equality, community cohesion and crime implications**

15.1　N/A

16　　**Equality Impact Assessment Completed**

16.1　No, as a result of an EIA screening it was determined that a full EIA was not required.

17　　**Key Decision**

17.1　No

18　　**Key Decision Reference**

18.1　N/A

19   **Background Papers**

19.1   The following is list of background papers on which this report is based in accordance with the requirements of Section 100(1) of the Local Government Act 1972. It does not include documents which would disclose exempt or confidential information as defined by the Act:

        File Ref: Background papers are included in Appendix 1
        Officer Name: Barbara Mulvihill
        Contact No   0161 770 1311

20   **Appendices**

20.1   Appendix 1 - Information Security Breaches by Directorate 2019-2020

Information Security Breaches by Directorate 2019-2020

Directorate	Quarter 1 Apr – Jun 2019	Quarter 2 Jul – Sep 2019	Quarter 3 Oct – Dec 2019	Quarter 4 Jan – Mar 2020	Total by Directorate
Chief Executive & Legal Services	3	0	0	0	3
Children's Services	8	8	7	9	32
Commissioning	3	0	8	3	14
Community Services & Adult Social Care	7	2	8	6	23
People and Place	2	4	2	2	10
Reform	6	7	0	2	15
Others	1	1	0	4	6
Total	**30**	**22**	**25**	**26**	**103**

Incidents can be categorised as follows:

- 59 instances of information being disclosed in error

- 18 instances of stolen / lost / misplaced records or equipment

- 5 instances of technical failure

- 17 instances of unauthorised access/disclosure

- 2 instances of uploading to a website/system in error

- 2 minor issues