Director: Angela Taylor
Author: Adam Grindrod (IG Officer) / Caroline Allen (Head of Legal & Governance Services)

Report to:	Governance and Audit Committee
Date:	25 January 2018
Subject:	GDPR Update

1 Purpose

1.1 To provide an update on the approach that WYCA has developed, to ensure compliance and readiness prior to the implementation of the General Data Protection Regulation (GDPR) on 25 May 2018.

2 Background

2.1 A key consequence of the 'One Organisation' programme of bringing together the different arms of the previous Integrated Transport Authority and Metro, WYCA and the LCR Enterprise Partnership officer structure into a consistent and cohesive corporate body has been the need to roll out a corporate set of policies and processes that work effectively for all parts of the business. Information governance (IG) in its broadest sense underpins this and is an area that has been identified as requiring development to reflect the aims and needs of the new organisation. A high level largely desk top IG assessment was undertaken in 2016 by Leeds City Council in partnership with WYCA officers in order to provide a baseline for a more focussed piece of work.

2.2 This piece of work in turn resulted in the establishment of an IG Project Team which has led on this agenda, implementing a number of more immediate actions (referenced further below) including the commissioning of a more detailed IG audit in June/July 2017 to assess not only WYCA's IG generally but also the actions needed in preparation for the implementation of GDPR. This audit concluded with a total of 55 recommendations for change/improvement and also resulted in the production of a high level Information Asset Register which for the first time sets out in one document all of the primary sets of information held across the organisation. This is a significant piece of work which provides the foundations for many of the tasks required on the lead up to GDPR.

3 Overview of Roles and Responsibilities

3.1 The Resources Director is WYCA's appointed Senior Information Risk Officer (SIRO) who is championing information risk within the organisation, to reinforce to all employees the importance of Information Governance and encourage the Leadership Team and Senior Managers to do likewise. The SIRO role has also been incorporated

into the Risk Management strategy and governance structure, to establish and maintain an appropriate risk appetite with proportionate boundaries and tolerances.

3.2 In addition, further resource has been created within the Legal & Governance Services team through the introduction of the role of IG Officer (appointed January 2017) and the role of Data Protection Officer for which an appointment has been made and the post will be taken up on 19 February 2018. This latter post will be responsible for developing and overseeing the CA's Information Governance strategy and its implementation, and will lead on ensuring compliance with GDPR requirements.

3.3 All Heads of Service (i.e. senior managers who report to a Director) have been appointed Information Asset owners, responsible for all information and assets obtained, managed, processed and held by WYCA. In addition, GDPR compliance and Information Governance is now a standing agenda item on the Heads of Service Monthly meeting.

3.4 Leadership Team also receive regular progress reports and the IG project is monitored by the One Organisation Programme Board as a key corporate project.

4 GDPR – Key Actions to Date

4.1 Significant preparatory steps have been taken to date, although it is recognised that there is further work to do. The two appendices to this report seek to provide an update albeit at a high level as to the current state of readiness at the present time, Appendix 1 is an extract from a document produced by the Information Commissioner's Office (ICO) which breaks down the tasks into 12 areas of focus. The table attached as Appendix 2 to this report provides an overview of the key actions taken to date and those yet to be undertaken assessed against each of the 12 ICO headings. Sitting behind this overview is a detailed action plan, based on the 55 recommendations of the IG Audit, with owners and target dates etc. owned and monitored by the IG Project Team and reported on to the One Organisation Board.

4.2 Significant steps taken to date which are worth highlighting include the following:-

4.3 The Information Asset Register has been developed since its initial production in July 2017 and is now designed to check and record GDPR compliance in programmes, projects and service areas. This will enable the appointed Data Protection Officer to complete a full gap analysis to ensure compliance when GDPR comes into effect in May 2018. This includes: Privacy Notices, Right to Erasure, Consent Wording, Privacy Impact Assessment, Children's Data, Data Breach and Incident reporting, Information Sharing Agreements and Data Processing Agreements. It is intended that this tool will provide a central location to act as the primary evidence base in relation to changed working practices. Guidance is currently being developed to roll out to Information Asset Owners (namely Heads of Service) to ensure that the organisation as a whole understands the new responsibilities that will flow from GDPR and plays

its part in embedding the changed practices and new processes into business as usual.

4.4 A suite of Information Governance related policies have been adopted and implemented across the organisation within the last 9 months including:-

- Data Protection Policy
- FOI and EIR Policy/Process
- Information Governance Policy
- Information Sharing Policy
- Subject Access Request Policy/Process
- Records Management, Retention and Disposal Policy
- Data & Systems Security Incident policy

4.5 Mandatory data protection training was rolled out for all employees between June and September 2017 and the new starter's induction process has been revised to ensure data protection training is undertaken within 2 weeks of commencing employment.

4.6 A series of exercises to raise awareness of GDPR implications continue to be rolled out to employees to remind them of their responsibilities to protect data and assets, highlight the risks to information assets and to embed a culture whereby employees can identify and understand the consequences and impacts of information losses or data breaches.

4.7 A process of reviewing and destroying information which the organisation should no longer hold is underway in relation to archived information and a relationship has been established with the West Yorkshire Archive Service resulting in the transfer of a significant amount of hard copy information for permanent preservation with future transfers agreed.

4.8 A dedicated Information Governance intranet mini-site is about to be launched which provides clear guidance on defining personal data and the importance of protecting it. The site signposts to Information Governance policies, clear and concise guidance on roles and responsibilities and holds an array of support and guidance available including links to the ICO website. The site also provides GDPR check lists and contacts in the ICT team and Information Governance Officer for direct, bespoke GDPR advice. Any measures or changes carried out to the site will be monitored, recorded and audited by the Information Governance Officer and will enable any new notices and agreements to be stored centrally for quick reference, in preparation for any audit, either internal or by an external party, and all activity recorded in our Information Asset Register in one central record.

5 Further steps

5.1 As set out in Appendix 2, further work is still required between now and May and inevitably thereafter. The detailed action plan will be used to track progress and to monitor risk. It is recognised that the additional expertise and capacity of the Data

Protection Officer will provide an invaluable additional resource to ensure that the project continues at pace. One of the key early tasks for the DPO will be to use both the results from the Leeds City Council audit and the results from the Information Asset Register gap analysis to inform and develop future activity and ensure that WYCA's processes and procedures are GDPR compliant ahead of 25 May 2018. Ongoing monitoring and control of Information Risks will take place via the Risk Management Strategy and Corporate Risk Register.

6 Financial Implications

6.1 Following the gap analysis by the Data Protection Officer, any additional resource needed to ensure GDPR compliance will be determined. Potentially this could involve short term external support to fully review systems and procedures to ensure risks are minimised and prevent potential fines by the ICO for data protection breaches, which as of 25 May 2018, could be up to €20 Million.

7 Legal Implications

7.1 Non-compliance with the GDPR could potentially lead to personal data being processed unlawfully which could lead to claims against the organisation, as well as reputational damage.

8 Staffing Implications

8.1 No additional impact. New roles in place.

9 External Consultees

9.1 None although Leeds City Council has provided support/critical friend input as identified in the report.

10 Recommendations

10.1 That Governance and Audit Committee note the approach that WYCA has developed, to ensure compliance and readiness prior to the implementation of the General Data Protection Regulation (GDPR) on 25 May 2018 and provide any feedback on this.