General Data Protection Regulation (GDPR)

Committee considering report:	Overview and Scrutiny Management Commission
Date of Committee:	9 January 2018
Portfolio Member:	Councillor Graham Bridgman
Date Portfolio Member agreed report:	21 December 2017
Report Author:	Robert O'Reilly
Forward Plan Ref:	n/a

1. Purpose of the Report

1.1 To update OSMC on the project to ensure compliance with the GDPR on 25th May 2018. The outline project plan was approved by Corporate Board on 16th May 2017. This report will describe what has already been achieved and what will be achieved to ensure compliance and minimise risk.

2. Recommendation

2.1 That OSMC note progress on the project.

3. Implications

3.1	**Financial:**	£6,500 for e-learning on GDPR for all staff (not schools) and £1,755 p.a. for LGA toolkit on record retention.
3.2	**Policy:**	See report for details.
3.3	**Personnel:**	None.
3.4	**Legal:**	GDPR will be a legal requirement from 25th May 2018.
3.5	**Risk Management:**	The likelihood of data security breaches will be lower (due to more training) but the potential consequences will be much higher (due to higher fines).
3.6	**Property:**	None.
3.7	**Other:**	None.

4. Other options considered

4.1 None

Executive Summary

5. Introduction / Background

5.1 There are Member Development Sessions on 29th January and 12th February 2018 to explain the GDPR in detail. This report provides assurance to OSMC that the Council has a project plan in place to ensure compliance with the GDPR from 25th May 2018. The project plan does not include schools (schools have their own Data Protection Officers and are taking steps to be GDPR compliant with guidance and support from Thomas Ng in Education).

5.2 The first report on the GDPR went to Corporate Board on 16th May 2017. The report was written by David Lowe (Corporate Programme Manager) before Robert O'Reilly was asked by Nick Carter to become Project Manager for GDPR compliance. The GDPR project has been running since September 2017 and will end on 31st August 2018. The last three months of the project will focus on evaluating the impact of the GDPR on WBC in light of the training and changes made as part of the project.

5.3 This project is part of the Corporate Programme and progress is also reported to the Corporate Programme Board by David Lowe. There is Member representation on the Corporate Programme Board.

5.4 The request for an update from OSMC provides a useful opportunity to revisit the original Corporate Board report to identify what has been done already and what there is still to do to meet the Information Commissioner's Office advice on how to achieve compliance with the GDPR.

5.5 The CB report set out 11 steps identified by the Information Commissioner's Office (ICO) for compliance with the GDPR. This report describes **progress to date** and actions that are **still to do** to ensure compliance with each of the ICO's 11 steps. The actions described have/will be undertaken mainly by James Gore (DPO) and Robert O'Reilly (Project Manager) with support from the rest of the project team (David Lowe and Kevin Griffin).

5.6 The ICO's 11 steps were as follows:

(1) "*A PR campaign and specific awareness sessions, in particular for senior managers, but also possibly including Staff Training sessions".*

(a) **Progress to date**: report to Corporate Board 16/06/17; discussion at Corporate Management Team 06/09/17; presentations to all SMTs (various dates); Reporter article on GDPR (October); discussions with Cllrs Bridgman and Cole (10/11/17 and 08/12/17); staff briefings attended by 252 employees (six briefings in December).

(b) **Still to do**: Member Development sessions (29/01/18 and 12/02/18) roll out of mandatory e-learning on GDPR for all staff from March 2018 with additional modules for staff with particular data processing duties.

(2) *"An information audit*". The project team decided that an information audit (internal or external) of existing personal data held by the Council was not required at the outset of the project because, if the Council was already compliant with the Data Protection Act, the potential risk

did not justify the cost involved. However, as part of the project Heads of Service will be auditing where and how personal data is processed in their services.

(a) **Progress to date**: Heads of service have been asked to identify one or more “GDPR champions” and to check that they are compliant with existing policies on data protection.

(b) **Still to do**: Heads of Service and their GDPR champion will meet with James Gore (Data Protection Officer) and Robert O’Reilly (GDPR Project Manager) in February 2018 to discuss existing level of compliance with the Data Protection Act and changes needed to be compliant with the GDPR. The main changes for Heads of Service to be aware of are the wording of ‘privacy notices’ (see below) and the need to undertake a Data Impact Assessment before undertaking any new project of installing any new IT system which will process personal data. The DPO has developed a template for services to use for their Data Impact Assessments which are an obligatory requirement under the GDPR.

(3) *“A review of all existing privacy notices*”. The project decided to roll out new privacy notices (aka ‘fair processing’ notices) rather than review existing privacy notices.

(a) **Progress to date**: the various briefings have explained what a GDPR compliant privacy notice needs to say; James Gore has developed a template privacy notice. A privacy notice needs to give the lawful basis for processing personal data. Please note: this will be explained in more detail at the Member Development Sessions. In a nutshell, there are six reasons which can be given on the privacy notice (they may overlap): CONSENT; CONTRACT; LEGAL OBLIGATION; VITAL INTERESTS; PUBLIC TASK; and LEGITIMATE INTERESTS.

(b) **Still to do**: work with services to insert the service specific reasons for processing personal data into the template privacy notice (from February).

(4) “*Deletion of historic data should be discussed with ICT (data outside retention schedule) and a process should be established for requests for personal data*.”

(a) **Progress to date**: services have been asked to review their retention schedules and how data is deleted when it is no longer required. There is an established process for dealing with requests for personal data which is operated by Strategic Support.

(b) **Still to do:** publish the retention schedule for the Council on the internet; work with ICT on possible technical solutions to deletion of out of date data.

(5) “*Revision of the Access to Information Policy to include the new individuals’ rights, along with the procedure covering access”.*

(a) **Progress to date:** the policy for staff on data protection is shown on the intranet (Strategic Support/Data Protection). The guidance document for staff has already been updated to show the current position and the position from 25th May 2018. The procedure for dealing with subject access requests will remain the same – Strategic Support will co-ordinate all responses working with relevant services.

(b) **Still to do:** the GDPR project will close on 31st August 2018. Between 1st June and 31st August 2018 the project team will evaluate the impact of the GDPR on subject access requests to see if the reduction in the time to respond under the GDPR from 40 days to one month has caused any operational problems; and to see if the abolition of the £10 fee has increased the number of data subject access requests coming into the Council. (Note: GDPR is separate from FOI requests. The GDPR is only about the privacy of personal data that can identify a living person, not all data or all information held by the Council).

(6) "*Examination of the various types of data processing WBC carry out, identify our legal basis for doing so and document it*."

(a) **Progress to date**: Strategic Support have registered the various types of data processing undertaken by the Council with the ICO under the existing DPA legislation. Under the GDPR, the reasons will not need to be registered with the ICO but must be made available to the ICO on request. This will be done by ensuring that all personal data collected by the Council is accompanied by a Privacy Notice which will be documented by the Data Protection Officer.

(b) **Still to do:** the legal basis for collecting personal data is currently subject to debate in networking circles of other councils. The DPO has recommended to the project team that WBC signs up with the LGA toolkit which gives service specific guidance on this subject. This is a subscription service costing £1,755 p.a. This request will be put to the Corporate Programme Board to secure the funding. The DPO and Project Manager have discussed the issue of "lawful basis for processing" in different networking groups and the key issue is how and when to seek *consent* for collecting and processing personal data. The GDPR gives specific rights to people who give consent for their personal data to be processed (for example the right to demand that processing of their data is halted). In councils this might not be possible to do (for example if we are collecting Council Tax or involved in a legal dispute). Therefore some councils are trying to limit their use of consent and expand the use of Privacy Notices which give a different legal basis for collecting personal data. The meeting with Heads of Service in February will focus on this issue and work on this will continue until early April.

(7) *"Review how consent is sought, obtained and recorded, and assess whether any changes are needed*".

(a) **Progress to date:** this links to (6) above and has been discussed at networking meetings.

(b) **Still to do:** discuss with Heads of Service how and why they need consent. Some councils seem to ne adopting a strategic position which limits asking for consent to very few circumstances where the individual wants something from the Council and it would have no adverse operational consequences if the person decided to withdraw their consent (for example, to join a e-mailing list to be notified of cultural events).

(8) *“Put into place systems to verify the ages of individuals we hold data for, and to gather parental or guardian consent for the data processing activity.”*

(a) **Progress to date: t**he DPO has raised this issue with relevant Heads of Service.

(b) **Still to do**: the GDPR provisions on this point were about children accessing social media sites (such as Face Book) and it is not clear how this provision will affect personal data processing on children for lawful council purposes which do not require consent. This is an aspect of the GDPR where WBC will follow the lead of the majority of other councils and LGA advice. The DPO will liaise with the Head of Education and the Head of C&FS on this issue in February.

(9) *“Ensure our procedures for detecting, reporting and investigating a personal data breach are robust and being followed”*

(a) **Progress to date:** this is not a change in the GDPR but the penalty for getting this wrong has been increased from a potential fine by the ICO of £100k to a potential fine of £17m (20m Euros). In WBC we have dealt with this risk by having mandatory data security training and a dedicated data security officer (Jackie Woodland).

(b) **Still to do:** the mandatory e-learning on the GDPR will reinforce the message to staff and managers that any data security breaches must be reported to Jackie Woodland without delay. Between 1st June and 31st August 2018 the project team will evaluate the impact of the GDPR on data security breaches. The main difference in the GDPR is that data security breaches must (rather than ‘should’) be reported to the ICO and reported under the GDPR within 72 hours where there is a risk of harm to the data subject.

(10) *Ensure WBC is able to demonstrate the technical and organisational safeguards for electronic data.*

(a) **Progress to Date:** the Head of ICT and Customer Services reported to Cllrs Cole and Bridgman on this issue on 10th November 2017. Kevin Griffin stated that all of WBC's personal data is held on systems in the Council's in-house data centres with the exception of the Locata choice based letting system used by Housing. There are very many controls in place for the protection of personal data. These controls are routinely examined as part of our annual re-accreditation to the Government's Public Services Network (PSN) code of connection. Internet of Things (IoT) devices are currently not deployed within the

Council. The Council uses many third party suppliers to provide infrastructure, services and systems. Controls have always been in place to control these suppliers' access to any personal data. We have several security systems in place including anti-virus/anti-malware software on all PCs and all servers. We have ransomware protection on servers. We have employer perimeter firewalls and application layer firewalls, web filtering and anti-spam filtering. All WBC laptops are encrypted. Only encrypted memory sticks are authorised for use in WBC. Encryption is used by our secure email system. All of our security systems send email alerts when breaches are detected. Alerts are sent by our systems on a 24x7x365 basis. The Council does not operate CCTV except for some limited use within the Council offices. PCs are patched automatically and 'silently' on an ongoing basis using our Microsoft System Centre Configuration Manager (SCCM). We use a scanning tool to regularly check for security vulnerabilities. We commission annual security penetration tests. Back office servers are patched at least quarterly during scheduled maintenance shutdown weekends. Backup tapes are held securely and data can only be restored by staff with appropriate authority and such restoration would be controlled by relevant policies**.**

(b) **Still to do:** Review **c**ontrols on suppliers' access to any personal data in the light of the GDPR requirements.

(11) **"***Designate a Data Protection Officer*".

(a) **Progress to date**: James Gore has been designated as the Council's Data Protection Officer. James is accredited with associate membership of the British Computer Society.

(b) **Still to do:** nothing on this point.

6. Proposal

6.1 There are no proposals in this report – it is for info to update OSMC.

7. Conclusion

7.1 This report has been requested by OSMC to provide assurance that the Council will be fully compliant with the GDPR on 25th May 2018. The conclusion of the report is that the Council is doing the right things as measured against the 11 steps (above) set out by the ICO. There is still work to do: meetings with Heads of Service to ensure compliance; networking with other Councils and the LGA to ensure that WBC is in the mainstream regarding any contentious issues (such as when to use consent); and mandatory e-learning for all staff (not schools) on the GDPR. Then there will be a further three months (June to August) when the project team will monitor the impact of the GDPR on the Council.

8. Appendices

8.1 Appendix A – Equalities Impact Assessment

Appendix A

Equality Impact Assessment - Stage One

We need to ensure that our strategies, polices, functions and services, current and proposed have given due regard to equality and diversity as set out in the Public Sector Equality Duty (Section 149 of the Equality Act), which states:

"(1) A public authority must, in the exercise of its functions, have due regard to the need to:

- ***(a) eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act;***
- ***(b) advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it; This includes the need to:***
  - ***(i) remove or minimise disadvantages suffered by persons who share a relevant protected characteristic that are connected to that characteristic;***
  - ***(ii) take steps to meet the needs of persons who share a relevant protected characteristic that are different from the needs of persons who do not share it;***
- ***(c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it, with due regard, in particular, to the need to be aware that compliance with the duties in this section may involve treating some persons more favourably than others.***

(2) The steps involved in meeting the needs of disabled persons that are different from the needs of persons who are not disabled include, in particular, steps to take account of disabled persons' disabilities.

(3) Compliance with the duties in this section may involve treating some persons more favourably than others."

The following list of questions may help to establish whether the decision is relevant to equality:

- **Does the decision affect service users, employees or the wider community?**
- **(The relevance of a decision to equality depends not just on the number of those affected but on the significance of the impact on them)**
- **Is it likely to affect people with particular protected characteristics differently?**
- **Is it a major policy, or a major change to an existing policy, significantly affecting how functions are delivered?**
- **Will the decision have a significant impact on how other organisations operate in terms of equality?**
- **Does the decision relate to functions that engagement has identified as being important to people with particular protected characteristics?**
- **Does the decision relate to an area with known inequalities?**
- **Does the decision relate to any equality objectives that have been set by the council?**

Please complete the following questions to determine whether a full Stage Two, Equality Impact Assessment is required.

What is the proposed decision that you are asking the Executive to make:	To comply with the GDPR
Summary of relevant legislation:	GDPR
Does the proposed decision conflict with any of the Council's key strategy priorities?	no
Name of assessor:	Robert O'Reilly
Date of assessment:	28/12/17

Is this a:		**Is this:**	
Policy	**Yes**	**New or proposed**	**Yes**
Strategy	**No**	**Already exists and is being reviewed**	**Yes**
Function	**No**	**Is changing**	**Yes**
Service	**No**		

1 What are the main aims, objectives and intended outcomes of the proposed decision and who is likely to benefit from it?	
Aims:	To comply with the GDPR
Objectives:	To comply with the GDPR
Outcomes:	To comply with the GDPR
Benefits:	To comply with the GDPR

2 Note which groups may be affected by the proposed decision. Consider how they may be affected, whether it is positively or negatively and what sources of information have been used to determine this.

(Please demonstrate consideration of all strands – Age, Disability, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion or Belief, Sex and Sexual Orientation.)

Group Affected	**What might be the effect?**	**Information to support this**
Age	Special category data is more protected under GDPR – applies to all categories below.	GDPR
Disability		

Gender Reassignment		
Marriage and Civil Partnership		
Pregnancy and Maternity		
Race		
Religion or Belief		
Sex		
Sexual Orientation		
Further Comments relating to the item:		
See GDPR on special category data (also known as sensitive data)		

3 Result	
Are there any aspects of the proposed decision, including how it is delivered or accessed, that could contribute to inequality?	**No**
Please provide an explanation for your answer:	
Will the proposed decision have an adverse impact upon the lives of people, including employees and service users?	**No**
Please provide an explanation for your answer:	

If your answers to question 2 have identified potential adverse impacts and you have answered 'yes' to either of the sections at question 3, or you are unsure about the impact, then you should carry out a Stage Two Equality Impact Assessment.

If a Stage Two Equality Impact Assessment is required, before proceeding you should discuss the scope of the Assessment with service managers in your area. You will also need to refer to the Equality Impact Assessment guidance and Stage Two template.

4 Identify next steps as appropriate:	
Stage Two required	no
Owner of Stage Two assessment:	
Timescale for Stage Two assessment:	

Name: Robert O'Reilly **Date: 28/12/17**

Please now forward this completed form to Rachel Craggs, Principal Policy Officer (Equality and Diversity) (rachel.craggs@westberks.gov.uk), for publication on the WBC website.