REPORT TO	ON
Governance Committee	14 March 2019

TITLE	REPORT OF
General Data Protection Regulation (GDPR) Update	Director of Customer and Digital

Is this report confidential?	No

1. PURPOSE OF THE REPORT

To update the Committee on GDPR progress to date and to seek comments on the Draft Data Protection Policy and Data Breach Policy, both of which incorporate changes as a result of GDPR.

2. RECOMMENDATIONS

Committee are requested to:

2.1 Note the progress to date in relation to GDPR and data breach policy.

2.2 Provide comments on the Draft policies so they can be refined and progressed to adoption through the appropriate approval process.

3. CORPORATE PRIORITIES

The report relates to the following corporate priorities:

Excellence and Financial Sustainability	X
Health and Wellbeing	
Place	

Projects relating to People in the Corporate Plan:

People	

4. BACKGROUND TO THE REPORT

4.1 The GDPR was introduced by the European Union (EU) on 25 May 2018 and works hand in hand with the Data Protection Act 2018. The law aims to give citizens more control over their personal data and to create a uniformity of rules to enforce across the continent.

4.2 The rise of new technologies has led to a massive increase in the amount of personal data that is collected, used, shared and stored. The GDPR aims to address this flow of personal data and to standardise the approach taken by all EU Member States GDPR applies to any organisation that handles personal data, including the Council, which handles data for residents and staff as part of its day to day business.

5. PROPOSALS (e.g. RATIONALE, DETAIL, FINANCIAL, PROCUREMENT)

5.1 In order to comply, an officer group have been following the guidelines issued by the Information Commissioners Office (ICO). An Officer group, who meet on a fortnightly basis have been working through an action plan which covers all relevant aspects of the Council operations to make changes to improve and ensure ongoing compliance.

An initial action log contained actions to be taken and this number has increased as the process evolved and the group identified areas that needed extra attention.

Actions have been split into 12 distinct categories

1. Awareness
2. Information audit and mapping
3. Communicating privacy information
4. Individuals rights
5. Subject Access Requests
6. Lawful basis for processing personal data
7. Consent
8. Children
9. Data Breaches
10. Data protection by design & Data Impact Assessments
11. Data protection Officer
12. International Data

The Plan is a live document and actions are being added at regular intervals. Great strides have been made by Officers in the last 12 months and as a result the Council is compliant in most areas with the exception of the following;

- Awareness – Staff have been made aware of the changes by way of Team briefs, articles on connect and a mandatory 4 module course on MILO. Of the 280 staff, 83% staff have completed the MILO modules (adjusted for absent staff and cleaning and grounds maintenance staff who do not have access to personal data). Plans are in place to raise awareness with these staff by other means and plans are in place to have an area on Connect dedicated to GDPR, with regular blogs, information and tips to maintain the profile of GDPR with staff.
- Data Protection by design - Procedures have been drawn up for creating data impact assessments and this is being rolled out as part of our Data Mapping exercises we are carrying out with departments on an ongoing basis. The Data Protection Policy has been refreshed and is attached for consideration.
- Data Breaches - A new policy has have been drawn up for consideration and is attached for consideration.

Further to the action taken above the Council will be at full compliance.

5.2 The Data Protection Policy was last reviewed in 2016 and so has been refreshed to take into consideration changes as a result of GDPR. The refreshed Policy is attached as an Appendix to this report for comment.

5.3 The Council has drafted a Data Breach Policy which is supported by procedural notes instructing Officers and Members what to do if they become aware of a data breach. Data breaches occur when, either accidentally or deliberately, an incident happens that may compromise the confidentiality, integrity or availability of systems or data which has caused, or has the potential to cause damage to the Council's data assets or reputation. Incidents can be many and varied but examples could be where data has been provided to the wrong customer, a system is hacked or a Council lap top is stolen. The Draft Data Breach Policy is attached as an Appendix to this report for comment.

5.4 Governance Committee are requested to note the progress made to date on GDPR compliance and to consider the draft policies and provide feedback. Any suggestions for improvement will be incorporated into the document to enable it to progress for approval.

5.5 Once approved, the Council will promote the policies to staff and improve staff awareness through Team briefs and Connect.

6. CONSULTATION CARRIED OUT AND OUTCOME OF CONSULTATION

6.1 **T**he Officer group have reviewed the documents before presentation to the Governance Committee.

7. FINANCIAL IMPLICATIONS

7.1 The only immediate financial costs of implication relate to training. The GDPR legislation means that the Council can potentially incur substantial fines as a result of non-compliance. This was demonstrated by the recent £44million fine imposed on Google when they contravened the legislation.

7.2 It is imperative therefore that the Council's policies and procedures surrounding Data Protection are robust and embedded within the organisation to minimise risk of data related incidents and the possible consequential fines.

8. LEGAL IMPLICATIONS

8.1 As above, non-compliance can also result in Legal challenges to the Authority, as well as loss of confidence in and reputational damage to the Council from residents, partners, peers and other stakeholders

9. COMMENTS OF THE STATUTORY FINANCE OFFICER

9.1 The adoption of GDPR policies mitigate the financial risk associated with holding data.

10. COMMENTS OF THE MONITORING OFFICER

10.1 The adoption of GDPR policies mitigates the financial and legal risk associated with holding data.

11. OTHER IMPLICATIONS:

▶ **HR & Organisational Development**	Training for GDPR is classed as 'mandatory' training for staff and a 'Data Essentials' module has been delivered to staff via the MILO system. Compliance is managed by HR
▶ **ICT / Technology**	ICT are currently working on refreshing the Information Security Policy relating to physical security of systems and relevant data contained within them

▶ **Property & Asset Management**	Not applicable
▶ **Risk**	As highlighted above. The risk is very real that data can be compromised so the Council needs to have a robust policy, supported by procedures and training to mitigate the risk and the major financial implications.
▶ **Equality & Diversity**	Not applicable

12. BACKGROUND DOCUMENTS -There are no background papers to this report

13. APPENDICES -

Appendix A Data Protection Policy
Appendix B Data Breach Policy

Report Author:	Telephone:	Date:
Kevin Conway – Head of Customer Experience	01772 625575	14 March 2019