West Lindsey District Council
The Entrepreneurial Council

Corporate Policy and Resources Committee

Date: 12/4/2018

Subject: Data Protection Policy – GDPR Revision

Report by:	Director of Resources
Contact Officer:	Steve Anderson Data Protection Officer 01427 676652 steve.anderson@west-lindsey.gov.uk
Purpose / Summary:	The General Data Protection Regulation (GDPR) comes into force on 25 May 2018. This report requests that members approve the attached Data Protection Policy and it's supporting Data Breach Reporting Policy and Procedure for adoption.

RECOMMENDATION(S):

1. That members approve the revised Data Protection Policy and its supporting Data Breach Reporting Policy and Procedure for formal adoption.

2. Delegated authority be granted to the Director of Resources to make minor housekeeping amendments to the policies in future, in consultation with the chairman of the Corporate Policy & Resources committee and chairman of Joint Staff Consultative Committee (JSCC).

IMPLICATIONS

Legal: This report introduces new policies to comply with the General Data Protection Regulation (GDPR). GDPR will be brought into UK law by the Data Protection Bill (currently before Parliament) on or before 25 May 2018 at which time the Data Protection Act 1998 will be repealed.

Financial : FIN/162/18/SL

There are no financial implications arising from this report.

Please note that non-compliance with the General Data Protection Regulation (GDPR) could lead to fines of up to 20 million euros (approx. £17.5 million), or 4% of turnover for the preceding financial year, whichever is the greater.

Staffing :

None.

Equality and Diversity including Human Rights :

This report supports the rights and freedoms of all individuals by setting out West Lindsey District Council's policy for managing and protecting personal and special category personal data.

Risk Assessment: None.

Climate Related Risks and Opportunities :

N/A

Title and Location of any Background Papers used in the preparation of this report:

None.

Call in and Urgency:

Is the decision one which Rule 14.7 of the Scrutiny Procedure Rules apply?

i.e. is the report exempt from being called in due to urgency (in consultation with C&I chairman)	**Yes**		**No**	**x**

Key Decision:

A matter which affects two or more wards, or has significant financial implications	**Yes**		**No**	**x**

1 Introduction

1.1 On 25 May 2018 the General Data Protection Regulation (GDPR) will become law across all member states of the EU simultaneously. The GDPR represents the most significant change to privacy legislation in 20 years and strengthens the rights of living individuals in a complex digital age. The UK will need to comply with the GDPR while it is still a member of the EU and will still need to comply when it leaves in order maintain a level of adequacy for doing business with the EU.

1.2 The Council has been preparing for the change for 2 years and has put in place some of the changes necessary already. Much of the work has been hampered, however, by a lack of practical guidance but this has now started to be issued by the EU Article 29 Working Party (WP29) and by the Information Commissioner's Office (ICO).

1.3 This report introduces new versions of the Council's Data Protection Policy and the Data Breach Reporting Policy and Procedure which have been revised to comply with the provisions of the GDPR.

2 The Impact of the GDPR on the Council

2.1 The Council, because of the wide range of services it provides, can assume different roles when handling the personal data of staff and citizens. In some cases it will be a Data Controller and decide the purposes and method of processing. Sometimes it will be a Data Processor and process data on behalf of another Data Controller. The third role the Council can assume is that of a Joint Controller and share data with one or more other Data Controllers.

2.2 As well as strengthening the rights of individuals which will require us to process their data in a much more transparent and secure way, the GDPR introduces for the first time an explicit principle of accountability for Data Controllers. Article 5(2) of the Regulation states "the controller shall be responsible for, and be able to demonstrate compliance with, the principles [GDPR Article 5(1) a-f]". Failing to comply with the principles could lead to fines in extreme cases of up to 20 million euros (approx. £17.5 million), or 4% of turnover for the preceding financial year, whichever is the greater.

2.3 Unlike the Data Protection Act (DPA) 1998, Data Processors will also have some direct responsibilities under GDPR and may also be subject to fines if they don't act only on the instructions of the Data Controller who has appointed them.

2.4 The ICO expects Data Controllers and Data Processors to put into place comprehensive but proportionate governance measures and good practice tools, some of which, such as privacy impact assessments, are now legally required in certain circumstances.

3 The Data Protection Policy

3.1 The Data Protection Policy (Appendix 1) is the cornerstone of our Privacy Compliance Framework and introduces the concept of a Personal Information Management System (PIMS) to comply with British Standard 10012:2017. The Policy demonstrates our understanding of the existing legal framework and our commitment to comply with it.

3.2 The revised Version 4 at Appendix 1 builds on our existing Policy, introduces the key provisions of the GDPR, and sets out the Council's policy with regard to the Privacy Compliance Framework under the following main headings:

- Policy Statement
- Scope
- Objectives of the PIMS
- Related Policies
- Notification
- Responsibilities
- Background to the GDPR
- Risk Assessment
- Security of Data
- Rights of Data Subjects
- Right of Access to Data (Data Subject Access Requests)
- Disclosure of personal information about third parties
- Disclosure of personal information to third parties
- Information Sharing
- Data Quality and Integrity
- Retention and Disposal of Data
- Data Transfers
- Information Asset Register
- Complaints
- Exemptions
- Breach of the Policy
- Review of the Policy
- Appendix 1 - List of Abbreviations and Definitions used in this Document

4 The Data Breach Reporting Policy and Procedure

4.1 The GDPR introduces far stricter rules for reporting breaches than required under previous legislation. Under GDPR Article 33 all breaches which are likely to result in a risk to the rights and freedoms of individuals must be reported to the ICO within 72 hrs of the Council becoming aware of them. Article 34 requires the Council to communicate all breaches that are likely to result in a high risk to individuals to the affected data subjects "without undue delay". Failure to comply with Article 34 can result in a fine not exceeding 10 million euros or 2% of turnover for the preceding financial year, whichever is the greater.

4.2 The new version 3.0 of The Data Breach Reporting Policy and Procedure (Appendix ii of Appendix 1) sets out the Council's policy for responding to data breaches. It explains what constitutes a Personal Data Breach with examples, what actions to take to contain and recover from the breach, how to perform an investigation, and how to notify the ICO and affected data subjects if required.

4.3 Once formally adopted, comprehensive training will be provided to all staff to make sure that they can recognise a breach and take the appropriate reporting action. A mandatory requirement for contractors and third-parties who process Council data on our behalf to report breaches will be written in to the relevant data processing contracts, memorandums of understanding, or service level agreements.

5 Decisions Required

5.1 That members approve the revised Data Protection Policy and its supporting Data Breach Reporting Policy and Procedure for formal adoption.

5.2 Delegated authority be granted to the Director of Resources to make minor housekeeping amendments to the policies in future, in consultation with the chairman of the Corporate Policy & Resources committee and chairman of Joint Staff Consultative Committee (JSCC).