BRECKLAND DISTRICT COUNCIL

Report of:	**Mark Stinson – Shared Executive Manager for Governance and Data Protection Officer**
To:	**Overview & Scrutiny Commission – 31 May 2018** **Cabinet – 12 June 2018**
(Author:	**Mark Stinson Executive Manager for Governance and Data Protection Officer)**
Subject:	**Data Protection Policy**
Purpose:	**To consider a draft Data Protection Policy, Data Security Breach Procedure and Response Procedures for Data Subject Requests.**

Recommendation(s):

1. That the new draft Data Protection Policy, Data Security Breach Procedure and Response Procedures for Data Subject Requests be recommended to Cabinet for approval and adoption.

2. That it be recommended to Cabinet that the Shared Executive Manager and Data Protection Officer be authorised to make amendments to the Policy and Procedures so far as is necessary to reflect legislative changes, emerging guidance and to incorporate links to other relevant documents.

1.0 **BACKGROUND**

1.1 The new General Data Protection Regulation (GDPR) became effective from 25 May 2018. GDPR will also be supplemented by a new Data Protection Act – which is presently progressing through Parliament.

1.2 As members may recall, the Executive Manager for Governance and Data Protection Officer attended the meeting of the Overview and Scrutiny Commission meeting on 25 January 2018 to brief members on the impact of GDPR.

1.3 GDPR enhances the rights of individuals, giving them more control over their data. It also places enhanced obligations on organisations who control and/or process data. Some of the key changes brought about by GDPR are:

- Much bigger fines are permitted by GDPR. As well as fines, individuals can bring private legal proceedings for breaches.
- GDPR obligations must be placed on contractors if they are handling personal data for the council. Similarly, we will need to accept GDPR obligations if we provide services to third parties.
- Individuals get enhanced rights over their data – the main ones are:

  - to access their data more quickly. Individuals are entitled to request details and copies of personal data we hold on them. This now has to be provided within 30 days (previously 40).
  - to have inaccurate data corrected.
  - to be 'forgotten' – in other words to have their data deleted. This right does not apply to certain personal data, such as data we need to fulfil a statutory purpose (an example would be personal data required for Council Tax collection).
- If we hold data on the basis of consent, then that consent must be genuine and must be informed (so we cannot rely on pre-ticked boxes).
- We must appoint a Data Protection Officer (The Executive Manager for Governance is identified in the Constitution as the Data Protection Officer)
- We need to be more transparent about the data we hold – informing data subjects of the data we hold, how long we will hold it, whether we share it, what we use if for, etc. This is achieved in a number of ways, but in particular we are producing 'Privacy Notices' to tell individuals about how we are using their information.
- We now have an 'Accountability' duty. This means that we need to be able to evidence compliance. We are doing this by building an audit trail of training, new policies, new procedures, technical and organisational measures, privacy notices, and other key actions.

1.4 Appended to this report is a draft Data Protection Policy, Data Security Breach Procedure and Response Procedures for Data Subject Requests. These are mostly based on professional legal precedents, and then tailored for our use. There remain some gaps as we await enactment of the new Data Protection Act and receipt of further guidance. There will also be a need to cross reference other policies as these are created or updated (such as IT security policies). In light of this, members are asked to authorise the Executive Manager for Governance and Data Protection Officer to make amendments to the policy but only so far as is necessary to reflect legislative changes, emerging guidance, and to cross reference linked policies.

2.0 OPTIONS

2.1 Cabinet may be recommended to:

- Approve the Policy and Procedures as written
- Approve the Policy and Procedures with amendments
- Do nothing.

3 REASONS FOR RECOMMENDATION

3.1 Approval will ensure that the Council has a fit-for-purpose Policy to assist in compliance with GDPR.

4 EXPECTED BENEFITS

4.1 The introduction of changes under GDPR places a duty on all data controllers and data processors to deal with personal data in a lawful and diligent manner. By ensuring that there is a robust Data Protection Policy in place, the Authority will be well positioned to adhere to these new requirements.

5 IMPLICATIONS

In preparing this report, the report author has considered the likely implications of the decision - particularly in terms of Carbon Footprint / Environmental Issues; Constitutional & Legal; Contracts; Corporate Priorities; Crime & Disorder; Equality & Diversity/Human Rights; Financial; Health & Wellbeing; Reputation; Risk Management; Safeguarding; Staffing; Stakeholders/Consultation/Timescales; Transformation Programme; Other. Where the report author considers that there may be implications under one or more of these headings, these are identified below.

5.1 Constitutional & Legal

5.1.1 GDPR compliance is a legal requirement. Constitutionally, final approval of the Policy sits with the Cabinet.

5.2 Contracts

5.2.1 GDPR places obligation on Data Controllers to impose GDPR obligations on contractors.

5.3 Financial

5.3.1 Adoption of the Policy does not of itself have any financial implications. Clearly, compliance with GDPR does have financial implications.

5.4 Risk Management

5.4.1 Having a robust Policy and associated procedures helps the Council to evidence compliance (the 'accountability principle' under GDPR). This, together with proper use of the policy and procedures, will ensure that our data practices improve and our level of risk reduces.

6 WARDS/COMMUNITIES AFFECTED

6.1 All wards/communities are affected.

7 ACRONYMS

7.1 GDPR – General Data Protection Regulation

Background papers:-	None

Lead Contact Officer
Name and Post: Mark Stinson Executive Manager - Governance
Telephone Number 01775 764612
Email: mark.stinson@breckland-sholland.gov.uk

Key Decision: No

Exempt Decision: No

Appendices attached to this report:

Appendix A	Data Protection Policy (draft)
Appendix B	Data Security Breach Procedure
Appendix C	Response procedures for data subject requests under GDPR