| Appendices 2 |
|---|

NORTHAMPTON
BOROUGH COUNCIL

# CABINET REPORT

| Report Title | Corporate Data Protection Policy |
|---|---|

**AGENDA STATUS:** **PUBLIC**

| | |
|---|---|
| **Cabinet Meeting Date:** | 18th July 2018 |
| **Key Decision:** | No |
| **Within Policy:** | Yes |
| **Policy Document:** | Yes |
| **Directorate:** | Borough Secretary |
| **Accountable Cabinet Member:** | Councillor Jonathan Nunn |
| **Wards:** | All |

## 1. Purpose

1.1 To advise Cabinet about the General Data Protection Regulations and Data Protection Act 2018 that came into force in May 2018.

1.2 To present for approval the Council's replacement Corporate Data Protection Policy [Appendix 2].

1.3 To agree the process for future minor updates to the policy.

## 2. Recommendations

2.1 Approve the DRAFT Corporate Data Protection Policy 2018 [option 3.3.1].

2.2 Delegate authority to the Data Protection Officer in consultation with the Monitoring Officer to implement future minor version controlled amendments to the approved Corporate Data Protection Policy to ensure the policy remains current and reflects changes in guidance and best practice until such a time as the legislation is replaced and a new policy is required.

## 3. Issues and Choices

### 3.1 Report background

3.1.1 Recent changes in data protection legislation, (The General Data Protection Regulation 2016 (GDPR) and the UK's Data Protection Act 2018 (DPA 2018)), have triggered the need to replace the current Corporate Data Protection Policy.

3.1.2 The General Data Protection Regulation [*(EU) 2016/679*] (GDPR) strengthens and unifies data controls and protection for all individuals within the European Union (EU) simplifying the regulatory environment.

3.1.3 The Data Protection Act 2018 [*Chapter 12, 2018*] (DPA 2018) implements the GDPR and the Law Enforcement Directive (EU) 2016/680) into UK law.

3.1.4 The review of the previous 2010 Policy has been delayed whilst the legislative changes, first drafted in 2012, have been enacted. This process concluded when the DPA 2018 received Royal Ascent on 23rd May 2018 and the GDPR became enforceable on 25th May 2018.

3.1.5 GDPR and DPA 2018 introduce a number of new statutory requirements to Data Protection (DP) legislation which have been incorporated into the policy. These include:

3.1.5.1 New personal data and data processing definitions, data principles and enhanced rights for individuals (data subjects).

3.1.5.2 Changes to the obligations imposed on data processors including third party Data Processors.

3.1.5.3 Obligations to keep data processing records and to audit data processes.

3.1.5.4 The requirement to conduct Data Protection Impact Assessments (DPIA's) when enhancing/delivering systems and/or processes.

3.1.5.5 A statutory duty to investigate all data breaches and report significant breaches to the Information Commissioner.

3.1.5.6 The statutory role and function of the Data Protection Officer.

3.1.6 The Information Commissioners Office (ICO) has produced a Guide to the GDPR . This is a 'living' document updated regularly by the ICO. The Guide includes links to relevant sections of the GDPR, other ICO guidance and to guidance produced by the EU's Article 29 Working Party to help organisations comply with its requirements.

3.1.7 The policy incorporates the recent legislative changes and Information Commissioner guidance into Council policy. It complements the legislation framework and provides an effective internal personal data governance framework for employees and Members.

### 3.2 Issues

3.2.1 Staff awareness of DP issues will be further supported through roll out of training across the Council to mitigate against any possible data breaches and resultant sanctions or reputational damage.

### 3.3 Choices (Options)

3.3.1 Approve the replacement Corporate Data Protection Policy.

3.3.1.1 This will provide an effective framework for governing the Council's use of personal data.

3.3.1.2 It is a statutory requirement to adopt a policy. GDPR Article 24(2) requires '*the implementation of appropriate data protection policies by the controller* [the Council]*'*.

3.3.2 Reject the replacement Corporate Data Protection Policy.

3.3.2.1 There is a risk of significant financial and reputational damage if the new statutory requirements are not adopted into Council policy.

3.3.2.2 The risk of not having an appropriate policy in place would be that the Council is seen not to be taking the importance of privacy rights of individuals seriously.

3.3.2.3 Failure to adopt the new policy will result in the continuation of an outdated policy document that does not fully reflect current legislation and statutory requirements. Poor data practices and possible regulatory sanctions will result.

## 4. Implications (including financial implications)

### 4.1 Policy

4.1.1 This policy replaces the Council's existing Corporate Data Protection Policy (revised) approved by Council Leader delegation on 2nd December 2010 and the previous Data Protection Act 1998 Policy Statement approved by the Council's Executive on 11th March 2002.

### 4.2 Resources and Risk

4.2.1 The policy references the new sanctions for serious data breaches in GDPR Article 83 (6) and DPA 2018 section 157(5) which increase the maximum penalty for serious and large data breaches [non-compliance] from the current £500,000 to a new maximum of 4% of annual turnover or the Sterling equivalent of €20,000,000. Though these are potential maximum fines there is a risk of significant financial and reputational damage if the policy is not adopted and staff retrained.

4.2.2 GDPR Article 38(2) states *'The controller and processor shall support the Data Protection Officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.'*

4.2.3 There will be a requirement for all staff to attend data protection training relevant to their role. This will be conducted in house with the cost absorbed within existing budgets. However there may be a need to enhance the staff structure supporting GDPR and, if required, this will be presented to Cabinet via CMB.

**4.3 Legal**

4.3.1 Implementing the requirements of the GDPR is a legal obligation placed upon the Council. Failure to comply with the GDPR could result in financial redress from the Information Commissioners Office.

**4.4 Equality and Health**

4.4.1 Data protection supports equality and diversity policies and is not expected to impact negatively on protected groups. It is non-discriminatory legislation that provides many of the safeguards disability discrimination legislation relies on and compliments the Human Rights of individuals as enshrined within EU and UK law.

4.4.2 Whilst certain categories of information such as race and ethnicity, religious beliefs and sexual orientation receive further protection to ensure that the security of personal data is maximised, overall the changes require the Council to be more transparent in its use of personal data and proactive in respect of upholding and promoting individuals rights.

4.4.3 The policy has been evaluated under the Council's Equality Impact Assessment procedures.

**4.5 Consultees (Internal and External)**

4.5.1 The draft policy has been circulated to Heads of Service, Senior Managers and the Leader of the Council for review and comment. Their comments have been incorporated into the DRAFT policy for approval.

**4.6 How the Proposals deliver Priority Outcomes**

4.6.1 Good governance of personal data is vital for the Council to operate effectively. The information we hold is an asset. If we use it well it provides many opportunities as it helps to make the organisation more efficient, improves the services we offer and engenders trust to members of the public, business partners and staff.

4.6.2 Embedding of the policy will provide assurance to the residents of Northampton that personal data held by the Council will be used lawfully.

4.6.3 Failure to embed a replacement policy, incorporating changes driven by GDPR (2016) and DPA (2018), might result in significant financial redress and reputational damage. This has the potential to undermine the strategic governance underpinning Council services. The policy and supporting training will increase the focus on protecting personal data.

### 4.7 Other Implications

4.7.1 None

## 5. Background Papers

5.1 The Data Protection Act 2018
5.2 The General Data Protection Regulations 2016
5.3 ICO Guide to the General Data Protection Regulations

**Appendix 1 – Summary of the key policy changes**
**Appendix 2 – The draft Corporate Data Protection Policy**

**David Taylor**
**Data Protection Officer**
**8536**