

18 July 2017

## Policy, Projects and Resources Committee

### Data Protection Act 1998 - New Policies

**Report of:** *John Chance, Finance Director and Daniel Toohey, Head of Legal Services and Monitoring Officer*

**Wards Affected:** *All*

**This report is:** *Public*

#### 1. Executive Summary

- 1.1 All staff and Members of local authorities are obliged to comply with the Data Protection Act 1998 (the Act) which requires individuals' personal data we hold to be processed securely. Breaches of the Act can result in serious financial and reputational harm to both the Council and to those whose information we hold. The Information Commissioner has the power to issue penalties up to £0.5m in such cases. Recently, a local council was fined £150,000 for a data breach. To effectively manage these risks, the Council has engaged a locum information governance lawyer to review the Council's compliance with the Act. A key aspect of this ongoing work is to ensure relevant policies exist and that these are current and effective in helping to manage business risk. These policies are now presented for Members' consideration and approval.

#### 2. Recommendation(s)

- 2.1 **That the proposed six policies appended to this report be approved by Members.**
- 2.2 **That delegated authority be granted to the Senior Information Risk Officer (currently the s.151 officer) acting in consultation with senior officers, the Chair of the Policy, Projects and Resources Committee and Monitoring Officer to make any minor adjustments or in respect of any changes in law as necessary.**

#### 3. Introduction and Background

- 3.1 Compliance with the Data Protection Act is inescapable requirement for all local authorities. Those that have failed to embrace the principles and

proper practices of data protection, achieved through the adoption of meaningful policies, procedures, training and administration, thereby achieving effective 'cultural buy-in' by all staff and Members, have suffered significant financial and reputational harm following intervention by the Information Commissioner. The proposed measures and policies will reduce ongoing business risk to the Council.

- 3.2 Members should note that the Data Protection Act will be replaced by the General Data Protection Regulation (GDPR) in May 2018. This European legislation will continue to be adopted as UK law from next May. Measures to ensure compliance with the GDPR will be taken once the Council has appropriate compliance measures in place under existing legal requirements. Those measures include: adoption of relevant policies; training for all staff with access to personal data across the Council; ensuring appropriate administration procedures and staff are in place to support compliance and development of a dedicated, high profile intranet page on DPA matters.
- 3.3 In accordance with the Act, the Council is required to appoint a senior information risk officer (SIRO) whose role is to oversee and report to the Council compliance with the Act and, in due course, with the GDPR. The Council's s151 officer is the current SIRO. Working with the Monitoring Officer, the SIRO has undertaken a review of the policies and procedures required to ensure full compliance with all current and forthcoming legislative provisions.

#### **4. Issue, Options and Analysis of Options**

4.1 Members approval of the appended policies is sought to enable these policies to be communicated to all staff and Members across the Council at the earliest opportunity, as part of the ongoing programme to effectively manage related business risk and to ensure full cultural buy in from staff and Members to the principles of data protection. There are no other options available as an alternative to these statutory requirements.

4.2 There are six policy updates under consideration:

- Clear Desk Policy (Appendix A)
- Data Protection Policy (Appendix B)
- Information Security Policy (Appendix C)
- Privacy Notice Policy (Appendix D)
- Privacy Impact Assessment Policy (Appendix E)

- Consent Policy

(Appendix F)

## **5. Reasons for Recommendation**

- 5.1 To assist in achieving effective compliance with the requirements of the Data Protection Act, so enabling the Council to keep related business risk to a minimum.

## **6. Consultation**

- 6.1 Senior managers in the Council's Corporate Leadership Board have been consulted on and are aware of the need for these updated policies.

## **7. References to Corporate Plan 2016-2019**

- 7.1 With regard to the priority: 'Community and Health' this report supports businesses, safeguards public safety and enhances standards locally through risk-based regulatory compliance with the Data Protection Act 1998 and the forthcoming GDPR.

## **8. Implications**

### **Financial Implications**

**Name & Title:** John Chance, Finance Director, Section 151 Officer and Senior Information Risk Officer

**Email:** john.chance@brentwood.gov.uk

**Tel:** 01277 312542

- 8.1 The associated training costs to move the Council to a compliant position will be funded from the central training budget and the cost of the interim locum solicitor is being covered from existing resources.

### **Legal Implications**

**Name & Title:** Daniel Toohey, Head of Legal Services and Monitoring Officer

**Email:** daniel.toohey@brentwood.gov.uk

**Tel:** 01277 312860

- 8.2 Legal implications are contained in the body of this report

## **9. Background Papers: None**

## **10. Appendices to this report**

- Clear Desk Policy (Appendix A)
- Data Protection Policy (Appendix B)
- Information Security Policy (Appendix C)
- Privacy Notice Policy (Appendix D)
- Privacy Impact Assessment Policy (Appendix E)
- Consent Policy (Appendix F)

### **Report Author Contact Details:**

**Name:** Gary Cordes, Information Governance Lawyer

**Telephone:** 01277 312570

**E-mail:** [gary.cordes@brentwood.gov.uk](mailto:gary.cordes@brentwood.gov.uk)