TEWKESBURY BOROUGH COUNCIL

Report to:	Audit and Governance Committee
Date of Meeting:	23 March 2023
Subject:	Data Protection Policy Review
Report of:	Head of Corporate Services
Head of Service/Director:	Corporate Director
Lead Member:	Lead Member for Corporate Governance
Number of Appendices:	1

Executive Summary:

The Council is committed to compliance with the requirements of the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

The Council's Data Protection Policy sets out the legislative framework and principles that all Council staff and Members must follow when handling and processing personal data. The policy also outlines the roles, responsibilities, and governance arrangements in place to ensure the council continues to fulfil its obligations.

A review of the current policy has been carried out to incorporate changes to the UK data protection law, ensure it remains in line with legal requirements and reflects best practice.

Recommendation:

To recommend to the Executive Committee that the revised Data Protection Policy be APPROVED

Financial Implications:

None arising directly from this report.

Legal Implications:

The Council is legally required to comply with the Data Protection Act 2018 and the UK GDPR. Any non-compliance therefore gives rise to a number of risks. The proposed policy ensures that appropriate safeguards and arrangements are in place to mitigate these risks as far as reasonably practical. The Data Protection and Digital Information Bill 2022/23 is due to receive Royal Assent in due course (possibly in the summer of 2023) and this policy will require further review and possible amendment at that stage.

Environmental and Sustainability Implications:

None arising directly from this report.

Resource Implications (including impact on equalities):

None arising directly from this report.

Safeguarding Implications:

None arising directly from this report.

Impact on the Customer:

Having an up-to-date Data Protection Policy helps demonstrate to customers, as well as employees, suppliers and other third parties, that they can have trust in engaging with the Council and feel confident that their personal data will be safe. It also ensures that the duty to inform customers of their rights under data protection legislation is met.

1.0 INTRODUCTION

1.1 The Council's current Data Protection Policy was adopted in 2018. A regular review of the policy is necessary to ensure that it remains consistent with legal requirements, reflects best practice and continues to be fit for purpose.

1.2 Since the adoption of the current policy, there have been changes to the UK data protection law following the UK's withdrawal from the European Union. The provisions of the EU GDPR have been incorporated directly into UK law, now known as the UK GDPR. In practice, this has meant little change, the core data protection principles, rights and obligations have remained the same. However, it is prudent to ensure that this change is reflected in the policy.

2.0 DATA PROTECTION REQUIREMENTS

2.1 In delivering services, the Council collects, stores and processes personal data about its customers, service users, employees, suppliers and other third parties. The Council must therefore comply with all relevant legislation and maintain good practices in order to protect the personal data held.

2.2 There are seven key principles which lie at the heart of data protection legislation. Compliance with these principles is fundamental to good data protection practice and the basis for our approach to processing personal data. These are:

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality (security)
- accountability

2.3 There are a number of key risks to the Council if it fails to meet these requirements. An accidental or deliberate breach of data protection could lead to sanctions being imposed by the Information Commissioners Office (ICO), including substantial fines. There is also a risk of reputational damage as a direct result of any non-compliance.

2.4 The Data Protection Policy therefore helps to mitigate these risks by clearly setting out the Council's approach and acting as a point of reference for all staff and Members. It is the duty of all staff and Members to ensure that personal data held by the Council is handled in accordance with the policy.

3.0 MAIN UPDATES TO THE POLICY

3.1 It is important to carry out a regular review of the Council's data protection approach to ensure it is meeting legal requirements and reflecting best practice. The current policy is, subject to the following amendments, considered to be relevant and up-to-date:

- the inclusion of an introduction/ policy statement, setting out the Council's commitment to safeguarding personal data
- updating legislation referred to in the policy i.e. UK GDPR
- the inclusion of a definition of personal data
- reference to the data protection governance arrangements in place
- inclusion of the Council's new data request system.

4.0 CONSULTATION

4.1 None

5.0 ASSOCIATED RISKS

5.1 There are inherent risks associated with not having an up-to-date Data Protection Policy and any non-compliance with data protection legislation. These include both financial and reputational risks to the Council.

6.0 MONITORING

6.1 The Data Protection Officer will monitor this policy on an annual basis. Compliance with the policy will also be monitored by the Council's Information Governance and Security Board.

7.0 RELEVANT COUNCIL PLAN PRIORITIES/COUNCIL POLICIES/STRATEGIES

7.1 None directly but the policy underpins the Council's values.

Background Papers: Data Protection Policy 2018 (Audit Committee 18.07.18, Executive Committee 29.08.18)

Contact Officer: Head of Corporate Services
01684 272002 graeme.simpson@tewkesbury.gov.uk

Appendices: Appendix 1 – Data Protection Policy 2023