**CABINET**
**27 JUNE 2019**

# DATA PROTECTION POLICY

**Cabinet Member:** Cllr Nikki Woollatt
**Responsible Officer:** Catherine Yandle, Group Manager for Performance, Governance and Data Security

**Reason for Report:** To review the existing policy after the first year since the Data Protection Act (DPA) 2018 and GDPR became law.

**RECOMMENDATION(S): That the Data Protection Policy be approved and the next review date set for 3 years hence.**

**Relationship to Corporate Plan:** This policy supports good governance arrangements enabling confidence in delivery of the Corporate Plan.

**Financial Implications:** The Data Protection Policy does not have any financial implications itself rather the contrary if the DPA 2018 and GDPR are not complied with.

**Legal Implications:** Not complying with the DPA 2018 and GDPR would expose MDDC to enforcement action by the Information Commissioner's Office (ICO).

**Risk Assessment:** Approving the Data Protection Policy reduces the risk of enforcement action by the ICO.

**Equality Impact Assessment**: No equality issues identified for this report.

## 1.0 Introduction

1.1 The Data Protection Act 2018 received royal assent on 23 May 2018. This represented the first major change to data protection for personal data for 20 years and incorporated the requirements of the GDPR, the Law Enforcement Directive and other amendments such as changes to the powers of the ICO and enforcement.

1.2 As this was a significant change to the legislation it was agreed at Cabinet on 14 June 2018 that the policy would be reviewed after one year to ensure it was operating correctly.

1.3 In addition in the light of Brexit the opportunity has been taken to bring the implications to Cabinet's notice. This is dealt with in section 3.0.

## 2.0 The Policy

2.1 The policy was already based on best practice but reflected additional requirements which were now included in the legislation.

2.2 The main changes at the time were to the Principles in section 5, Special Category Data in section 6 and the Rights of Data Subjects in section 8.

2.3 There have been no further changes identified as being necessary after the first year of operation of the policy.

## 3.0 **Brexit and DPA 2018**

3.1 Under the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 GDPR becomes UK GDPR and references to the Union, the United Kingdom and Member state law, domestic law. There is also recognition of the “EU GDPR”.

3.2 The effect of all this is that the fundamental principles, obligations and rights that organisations and data subjects have become familiar with will stay the same. The regulations also transitionally recognise all EEA countries (including EU Member States) and Gibraltar as ‘adequate’ to allow data flows from the UK to Europe to continue. The Information Commissioner will remain the UK’s independent regulator for data protection.

3.3 For data transferred from the EEA on exit date the UK will be a third country outside the EEA. Under the GDPR, an EEA controller or processor will be able to make a restricted transfer of personal data to the UK if it is covered by an adequacy decision by the European Commission.

3.4 We now need to consider how we may continue to make and receive those transfers lawfully after exit date, and without an adequacy decision by the European Commission in relation to the UK. Key transfers to consider will be from the EEA to the UK but if the EEA sender has put in place one of the EU GDPR list of appropriate safeguards, the EEA sender will be able to make the transfer to us.

## 4.0` **Conclusion**

4.1 That the Data Protection Policy be approved and the next review date set for 3 years hence.

**Contact for more Information:** Catherine Yandle, Group Manager for Performance, Governance and Data Security

**Circulation of the Report:** Cabinet Member and Leadership Team