

Report to:	AUDIT PANEL
Date:	Tuesday 25 June 2024
Reporting Officer:	Carol McDonnell – Head of Assurance
Subject:	INFORMATION GOVERNANCE ANNUAL REPORT AND REFRESHED FRAMEWORK AND POLICIES
Report Summary:	This report presents the annual Information Governance Report and updated framework and policies in respect of Information Governance.
Recommendations:	<ol style="list-style-type: none"> 1. Members note the Information Governance Annual Report Appendix 1 2. Members approve the Information Governance Framework shown at Appendix 2. 3. Members approve the Data Protection Policy shown at Appendix 3. 4. Members approve the Appropriate Policy shown and Appendix 4. 5. Members approve the Social Media for Investigations Policy shown at Appendix 5. 6. Members approve the Subject Access Request Policy shown at Appendix 6. 7. Members approve the Freedom of Information Policy shown at Appendix 7. 8. Members approve the Records Management Policy shown at Appendix 8. 9. Members approve the Records Retention and Disposal Policy shown at Appendix 9.
Corporate Plan:	Strong information governance supports the individual operations, which deliver the objectives of the Council.
Policy Implications:	The documents will add further guidance to the Data Protection / Information Governance Framework to enable staff to adhere to the requirements of the Data Protection Act 2018 and UK General Data Protection Regulations (GDPR).
Financial Implications: (Authorised by the statutory Section 151 Officer & Chief Finance Officer)	<p>There are no direct financial implications arising from this report. However, it should be noted that there is a significant financial risk to the Council for non-compliance with the Data Protection Act 2018 and UK GDPR as this can result in the Information Commissioner's Office (ICO) imposing financial penalties.</p> <p>For context, these can be up to a maximum of £17.5 million or 4% of annual turnover (depending on which is larger) for the most serious breaches. In addition, data subjects impacted by data breaches can claim for damages, which can also result in a financial liability on the Council budget, the value of which will be dependent on the individual claim(s).</p> <p>The report and appendices reference relevant training for Council employees on the various policies as required. The related cost of</p>

the training will be financed via the Council's existing revenue training budget.

**Legal Implications:
(Authorised by the
Borough Solicitor)**

It is important that the Council's Information Governance policies are continually refreshed to ensure that the Council complies with its statutory obligations in this regard. Non-compliance with the Data Protection Act 2018 (as amended) and UK GDPR (General Data Protection Regulation) could expose the Council to enforcement action and/or financial penalties from the ICO, claims for damages from data subjects impacted by data breaches, as well as cause damage to the Council reputationally.

Risk Management:

Information is a valuable asset to the Council and personal information needs to be protected as privacy failures could be very damaging to the Council in terms of reputational damage and significant financial implications. The necessity to update and refresh the framework and policies is critical if we are to comply with the requirements of the Data Protection Act 2018 and UK GDPR.

Access to Information:

Not Confidential

Background Information:

The background papers can be obtained from the author of the report Carol McDonnell, Head of Assurance:

Telephone: 0161 342 3231

e-mail: Carol.McDonnell@tameside.gov.uk