Report To:	**AUDIT PANEL**
Date:	12 March 2024
Reporting Officer:	Carol McDonnell – Head of Assurance
Subject:	**INFORMATION GOVERNANCE POLICIES**
Report Summary:	This report presents the updated policies in respect of information governance.
Recommendations:	1. Members approve the IT Security Policy shown at **Appendix 1.** 2. Members approve the IT Acceptable Use Policy shown at **Appendix 2.** 3. Members approve the Social Media Use: Responsible Conduct Policy shown at **Appendix 3**.
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)**	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. For context, these can be up to a maximum of £17million 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).
Legal Implications: **(Authorised by the Borough Solicitor)**	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 damage the Council reputationally.
Risk Management:	Information is a valuable asset to the Council and personal information needs to be protested 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 policies that are part of the Data Protection / Information Governance Framework is critical if we are to comply with the requirements of the Data Protection Act 2018 and UK GDPR.
Access to Information:	The background papers relating to this report can be obtained by contacting Carol McDonnell, Head of Assurance ☎ 0161 342 3231 ✉ carol.mcdonnell@tameside.gov.uk

1. INTRODUCTION

1.1 Information Governance can mean different things to different people. It can be defined as the set of multi-disciplinary structures, policies, procedures, processes, and controls implemented to manage information, supporting the Council's immediate and future regulatory, legal, risk, environmental and operational requirements.

1.2 Information Governance can also describe the way we manage our obligations for: accessing information, reuse of information, records management, surveillance, data protection, information security, Information Technology (IT) security, etc.

1.3 The primary pieces of legislation relating to Information Governance and data protection are:

- Data Protection Act 2018 (DPA) – enables an applicant to access information of which they are the subject, e.g., someone's own education/social care records, employee files etc.

- UK General Data Protection Regulations (UK GDPR) – like the EU GDPR, provides safeguards to individuals over the processing of their personal information and setting requirements for organisations to ensure appropriate technical and organisational measures are in place to comply with the principles of data protection.

1.4 The following lists some other legislation that impacts Information Governance:

- Freedom of Information Act 2000 (FOIA) – enables an applicant access to information which is held by/on behalf of public authorities and those bodies carrying out a public function, and which does not fall under either of the access regimes i.e., personal information or environmental information.

- Environmental Information Regulations 2004 (EIR) – enables an applicant to access environmental information.

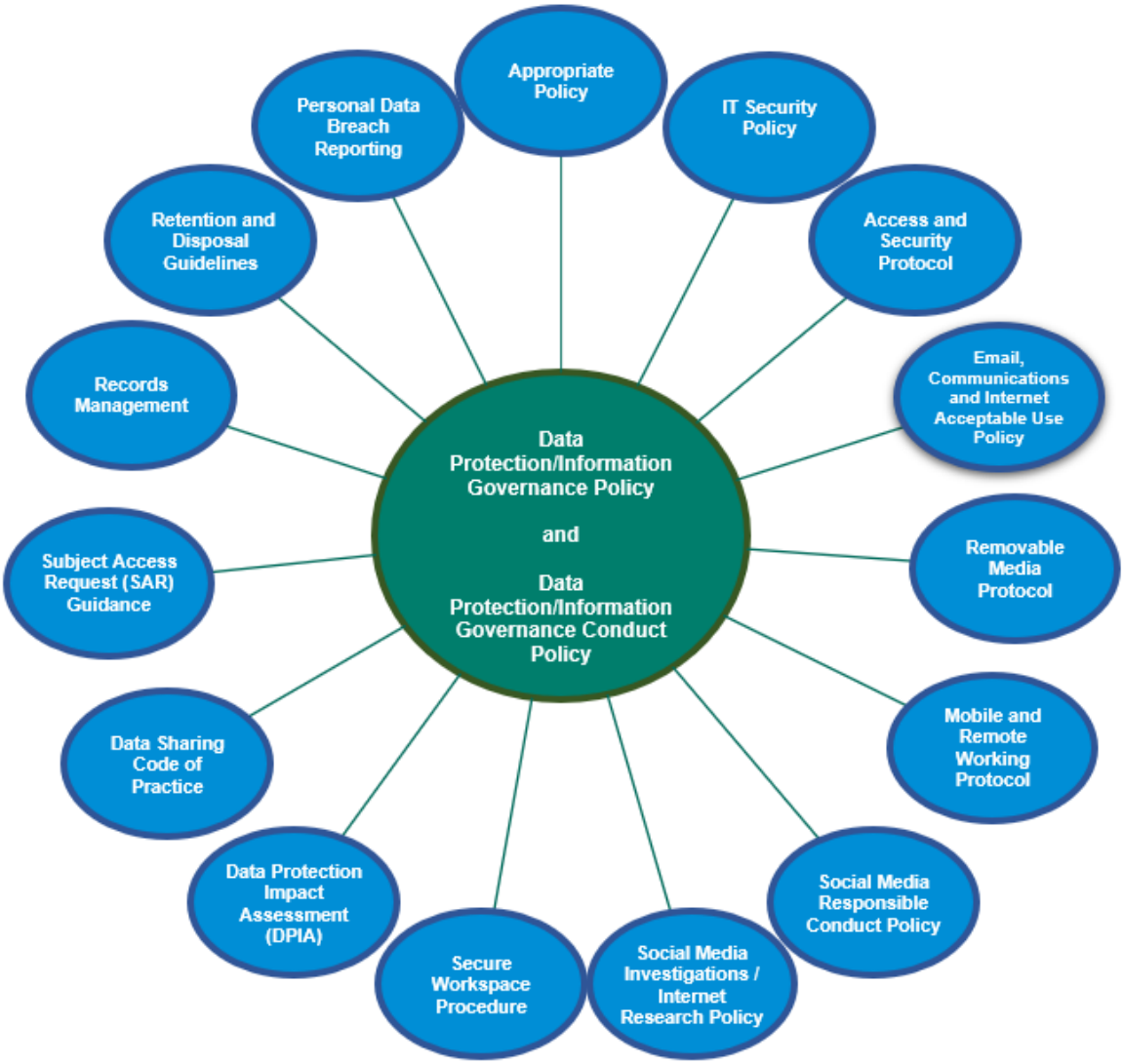
- Privacy and Electronic Communications Regulations 2003 (PECR) – sets out privacy rights relating to electronic communications, and covers electronic marketing, the use of website cookies, the security of public electronic communications services and privacy of users of electronic communications services.

- Re-use of Public Sector Information Regulations 2015 – establishes the UK framework for the re-use of public sector information. Accessible information which is produced, held, or disseminated by the public sector body must be made available for re-use (unless it is otherwise restricted or excluded).

2. DATA PROTECTION / INFORMATION GOVERNANCE FRAMEWORK

2.1 The Data Protection / Information Governance Framework comprises the policies and procedures of the Council, which relate to Information Governance, with the overarching document being the Data Protection / Information Governance Policy and the Data Protection / Information Governance Conduct Policy.

2.2 The following diagram details all the policies and procedures contained within the framework:



3. UPDATED FRAMEWORK DOCUMENTS

3.1 An Information Governance Workplan is in place, which is monitored by the Information Governance Group.

3.2 At the last meeting of the Information Governance Group, the following policies were reviewed:

- IT Security Policy – which sets out the Council's policy on using its IT equipment and its internal and external infrastructure. The policy is located at **Appendix 1**.

- IT Acceptable Use Policy – which sets out what the various Council's IT equipment can be used for, including permitted personal use, access controls, security, and compliance. The policy is located at **Appendix 2**.

- Social Media Policy – which sets out the expectations of officers and members in the use of social media as part of council duties as well as personal use. The policy is located at **Appendix 3**.

4. COMMUNICATIONS AND COMPLIANCE

4.1 Once the policies have been approved, steps will be taken to ensure that the new policies are effectively communicated to all staff, and to ensure compliance with policies is embedded.

4.2 It is proposed the Council takes the following steps:

4.3 Initial communications about the changes should be communicated through the Chief Executive's Weekly Briefing and posted on the Intranet outlining the key changes and what will happen as part of the user experience.

4.4 The log on screen 'Warning' message currently displayed at each log in will be updated to reflect the changes in this report. Users cannot log on without clicking OK to confirm their acceptance of the relevant policies.

4.5 A pop-up message will be displayed after signing in for the first time after the changes are implemented that will ask users to review the policies after providing a summary of the key changes. Users will be unable to progress further into the systems without indicating they have read and understood the policies and guidance.

4.6 Paper copies of the revised policies along with a paper briefing will be provided for all non-networked officers, e.g. officers based at the Depot at the same time as the system changes are made for IT users.

4.7 Lunch and learn sessions will be provided via Teams over a four-week period, allowing users multiple options to attend a live session. A similar session can be provided for non-networked officers if there is sufficient demand for one to be run.

4.8 One of the lunch and learn sessions will be recorded and uploaded to Me.Learning for any user that cannot attend the proposed sessions. It will also be available to new starters as part of the onboarding process during their probation periods.

5. RECOMMENDATIONS

5.1 As set out on the front of the report.