



<b>Report To:</b>	<b>AUDIT PANEL</b>
<b>Date:</b>	28 September 2021
<b>Reporting Officer:</b>	Kathy Roe – Director of Finance Wendy Poole – Head of Risk Management and Audit Services
<b>Subject:</b>	<b>DATA PROTECTION/INFORMATION GOVERNANCE UPDATE REPORT</b>
<b>Report Summary:</b>	The report provides an update on Data Protection / Information Governance across the Council and presents some key documents for approval.
<b>Recommendations:</b>	Members are asked to consider and note the report and: <ol style="list-style-type: none"> <li>1) Approve the Data Protection/Information Governance Policy attached at <b>Appendix 1</b>.</li> <li>2) Approve the Data Protection/Information Governance Conduct Policy attached at <b>Appendix 2</b>.</li> <li>3) Approve the adoption of the Data Sharing Code of Practice detailed in Section 3.4 of the report.</li> </ol>
<b>Corporate Plan:</b>	Strong information governance supports the individual operations, which deliver the objectives of the Council.
<b>Policy Implications:</b>	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).
<b>Financial Implications:</b> <b>(Authorised by the statutory Section 151 Officer &amp; Chief Finance Officer)</b>	Non-compliance with the Data Protection Act 2018 or the UK GDPR can result in the Information Commissioner's Office imposing financial penalties up to maximum of £17million or 4% of annual turnover (depending on which is larger) for the most serious breaches.
<b>Legal Implications:</b> <b>(Authorised by the Borough Solicitor)</b>	Non-compliance with the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR) could expose the Council to enforcement action and/or a financial penalty from the Information Commissioners Office as well as damage the Council reputationally.
<b>Risk Management:</b>	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 they could have significant financial implications. The necessity to update and refresh our Data Protection/Information Governance Framework is critical if we are to comply with the requirements of the Data Protection Act 2018 and UK GDPR.
<b>Background Papers:</b>	The background papers relating to this report can be inspected by contacting Wendy Poole.

 Telephone: 0161 342 3846

 e-mail: [wendy.poole@tameside.gov.uk](mailto:wendy.poole@tameside.gov.uk)

# 1. INTRODUCTION

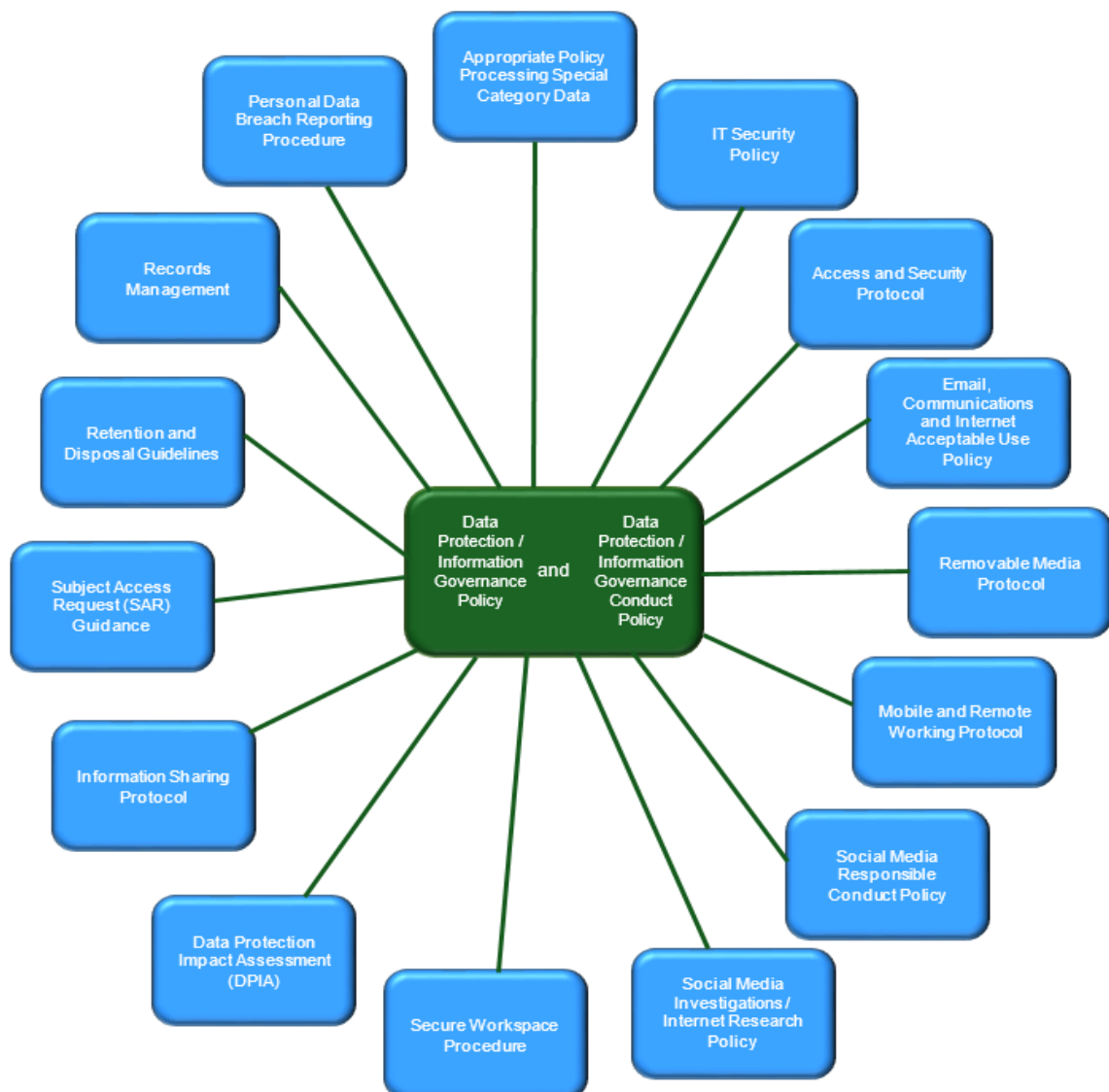
1.1 The primary pieces of legislation relating to information governance and data protection are the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) which came into force from 25 May 2018 and were update to UK GDPR following the UK's departure from Europe.

# 2 DATA PROTECTION/INFORMATION GOVERNANCE WORK PLAN

2.1 A work plan is in place which is monitored by the Information Governance Group to ensure that the Council continues to review its compliance with the Data Protection Act 2018 and UK GDPR.

2.2 A key task included in the plan is to review the Information Governance Framework, which is presented below. To align terminology with that used by the Information Commissioners Office, the Information Governance Group at its meeting on 7 September 2021 approved to update the name of the Framework to the "Data Protection/Information Governance Framework" which is detailed in Diagram 1.

**Diagram 1 – Data Protection/Information Governance Framework**



### 3 UPDATED FRAMEWORK DOCUMENTS

3.1 The Information Governance Group, chaired by the Data Protection Officer considered three documents at its meeting on 7 September 2021 that need to be approved by the Audit Panel. Consultation has taken place with the Information Governance Champions and feedback has been incorporated into the versions attached in Appendices 1 and 2.

#### 3.2 **Data Protection/Information Governance Policy**

3.2.1 This policy is the overarching document of the Council's wider Data Protection/Information Governance Framework and underpins all other elements of the framework.

3.2.2 The document attached at **Appendix 1** is an update on the existing policy, which has been refreshed to clarify the principles of data protection and the various roles and responsibilities across the Council. The definitions relating to personal and special category data have been expanded to incorporate the various formats in which data can be held. The policy also now sets out the key data protection principles set out in UK GDPR and the responsibilities placed on the Council as an organisation.

3.2.3 Further detail has been added around the issues of data/information sharing and the need to consider fully the risks of all data processing activities, including conducting a Data Protection Impact Assessment where necessary to minimise the risk to the data subjects involved, the Council's customers, residents and service users. The policy now sets out the rights of data subjects, in particular Subject Access Requests, and the obligations placed on the Council.

3.2.4 The updated policy covers:

- Introduction;
- Purpose of Policy Statement;
- Data Protection/Information Governance Framework;
- Scope
  - Definitions;
  - Data Protection Principles;
  - Personal Information Sharing;
  - DPIA
  - Consent;
  - Data Subject Rights and SAR;
  - Training;
- Data Protection/Information Governance;
- Responsibility for Information Governance.

#### 3.3 **Data Protection/Information Governance Conduct Policy**

3.3.1 In order for the Council to demonstrate that it is compliant with the Data Protection Act 2018 and UK GDPR it needs a robust set of policies and procedures to ensure it is handling data safely and appropriately and that all employees are aware of their role in ensuring data protection and dealing with the rights of individual data subjects.

3.3.2 This policy sits at the heart of the Data Protection/Information Governance Framework and provides an overview of each supporting framework document as well as setting out the key conduct issues for managers and employees to be aware of and highlights best practice as well as actions which may breach the policies and/or breach individual data subjects' rights.

3.3.3 This policy can function as a quick reference guide on some of the key points, but is to be read in conjunction with the other framework policies and contains an appendix setting out the mandatory documentation that employees in a variety of roles need to review and comply with.

- 3.3.4 The document attached at **Appendix 2** is an update on the existing policy and has been refreshed to clarify the principles of data protection and the various roles and responsibilities across the Council. It now reflects the current legislative and regulatory guidance and better communicates the role of the Information Governance Team and the internal procedures it has put in place.
- 3.3.5 Appendix 1, of the Policy provides a brief summary of the other framework documents, has been updated to include several new policies which have been or are in the process of being added to the Data Protection/Information Governance Framework. It covers the 'key conduct issues' for each of the framework documents by breaking it down into acceptable and unacceptable conduct, which will make matters clearer for the employees and managers reading the policy and give clear guidance on the standards to be upheld across the Council.
- 3.3.6 Appendix 2 has been streamlined and presents the documents critical to the various roles across the Council.
- 3.3.7 The updated policy covers:-
- Introduction;
    - Definitions;
  - Procedures;
  - Roles and Responsibilities;
    - Manager responsibilities;
    - Employee responsibilities;
  - How we manage breaches of the policy;
  - Appendix 1 – Data Protection/Information Governance Framework;
    - Data Protection/Information Governance Policy and Conduct Policy;
    - Appropriate Policy Processing Special Category Data;
    - IT Security Policy;
    - Access and Security Protocol;
    - Email, Communications and Internet Acceptable Use Policy;
    - Removable Media Protocol;
    - Mobile and Remote Working Protocol;
    - Social Media Responsible conduct Policy;
    - Social Media Investigations/Internet Research Policy;
    - Secure Workspace Procedure;
    - Data Protection Impact Assessment (DPIA);
    - Information Sharing Protocol;
    - Subject Access Request (SAR) Guidance;
    - Records Management Policy;
    - Retention and Disposal Schedule;
    - Personal Data Breach Reporting Procedure;
  - Appendix 2 – Data Protection/Information Governance Framework Mandatory Documents Matrix.

## 3.4 **Data Sharing Code of Practice**

- 3.4.1 In 2011 the Information Commissioner's Office (ICO) published its first Data Sharing Code; since then the type and amount of data collected by organisations has changed enormously, as has the technology used to store and share it, and even the purposes for which it is used.
- 3.4.2 The UK Information Commissioner, accepts that data is one of modern society's greatest assets. Ready access to information and knowledge, including about individual citizens, can lead to many economic and social benefits, including greater growth, technological innovations and the delivery of more efficient and targeted services.

3.4.3 The updated Data Sharing Code of 2021 has been written to give individuals, businesses and organisations the confidence to share data in a fair, safe and transparent way in this changing landscape. This code is aimed at giving practitioners the practical steps they need to take, to share data while protecting people's privacy.

3.4.4 In her introduction to the new code the Information Commissioner states:  
"I have seen first-hand how proportionate, targeted data sharing delivered at pace between organisations in the public, private and voluntary sectors has been crucial to supporting and protecting the most vulnerable during the response to the COVID-19 pandemic. Be it through the shielding programme for vulnerable people, or sharing of health data in the Test and Trace system. On a local and national level, data sharing has been pivotal to fast, efficient and effective delivery of pandemic responses.

Utilising the data we collectively hold and allowing it to be maximised properly will have economic benefits. Data sharing that engenders trust in how personal data is being used is a driver of innovation, competition, economic growth and greater choice for consumers and citizens. This is also true in the sphere of public service delivery where efficient sharing of data can improve insights, outcomes and increase options for recipients".

3.4.5 This code demonstrates that the legal framework is an enabler to responsible data sharing and busts some of the myths that currently exist. However, the code of practice will not solve all the challenges for data sharing. There are other barriers to data sharing, including cultural, technical and organisational factors. Overcoming these will require more than just the ICO; it will require a collective effort from practitioners, government and the regulator.

3.4.6 The Commissioner and the ICO see the publication of this code not as a conclusion but as a milestone in this ongoing work. The ICO will continue to provide clarity and advice in how data can be shared in line with the law. This code, and the products and toolkits published alongside it, provides a gateway to good data sharing practice and the benefits we can expect from the results.

3.4.7 This is a statutory code of practice made under Section 121 of the Data Protection Act 2018. It is a practical guide for organisations about how to share personal data in compliance with data protection law. It aims to give organisations the confidence to share data fairly and proportionately.

3.4.8 Data protection law enables fair and proportionate data sharing:-

- Data protection law facilitates data sharing when you approach it in a fair and proportionate way.
- Data protection law is an enabler for fair and proportionate data sharing, rather than a blocker. It provides a framework to help you make decisions about sharing data.
- This code helps you to balance the benefits and risks and implement data sharing.
- Data sharing has benefits for society as a whole.
- Sometimes it can be more harmful not to share data.
- When considering sharing data:
  - you must comply with data protection law;
  - we recommend that you assess the risks using a Data Protection Impact Assessment (DPIA); and
  - it is good practice to have a data sharing agreement.
- When sharing data, you must follow the key principles in data protection legislation:
  - The accountability principle means that you are responsible for your compliance, and you must be able to demonstrate that compliance.
  - You must share personal data fairly and transparently.
  - You must identify at least one lawful basis for sharing data before you start any sharing.
  - You must process personal data securely, with appropriate organisational and technical measures in place.

- In your data sharing arrangement, you should have policies and procedures that allow data subjects to exercise their individual rights easily.
- You can share data in an emergency, as is necessary and proportionate. Examples of an emergency situation are the risk of serious harm to human life, or the immediate need to protect national security.
- You may share children's data if you can demonstrate a compelling reason to do so, taking account of the best interests of the child.
- The government has devised a framework for the sharing of personal data, for defined purposes across the public sector, under the Digital Economy Act 2017 (DEA).

3.4.9 The Code of Practice was laid before Parliament on 18 May 2021 for 40 Sitting Days. Information from the ICO suggests that this period has now elapsed and the code will shortly be issued by the Information Commissioner.

3.4.10 The Code is available on the ICO Website using the link below.

<https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/>

3.4.11 The Code covers the following areas:

- Information Commissioners Forward
- Executive Summary
- Navigating the data sharing code
- About this code
- Data sharing covered by the code
- Deciding to data share
- Data sharing agreements
- Data protection principles
- Accountability
- Fairness and transparency in data sharing
- Lawfulness
- Lawful basis for sharing personal data
- Security
- The rights of individuals
- Law enforcement processing
- Due diligence
- Sharing personal data in databases and lists
- Data sharing and children
- Data sharing in an urgent situation or in an emergency
- Data sharing across the public sector: the Digital Economy Act codes
- Enforcement of the code
- Glossary
- Annex A – Data Sharing Checklist
- Annex B – Data sharing request form template
- Data sharing decision form template
- Annex C – Case Studies

3.4.12 In practical terms the introductory information in this report will be added to the Data Protection/Information Governance Framework, together with the link to the ICO Data Sharing Code of Practice, so that any updates by the ICO are visible to the user. Support and advice will be provided by the Information Governance Team.

## 4 RECOMMENDATIONS

4.1 As set out on the front of the report.