Report To: **AUDIT PANEL**

Date: 15 March 2022

Reporting Officer: Kathy Roe – Director of Finance

Wendy Poole – Head of Risk Management and Audit Services

Subject: **DATA PROTECTION / INFORMATION GOVERNANCE UPDATE REPORT**

Report Summary: The report provides an update on Data Protection/Information Governance across the Council and presents some key documents for information.

Recommendations: Members are asked to:

1) Note the report.
2) Approve the Subject Access Request Guidance attached at **Appendix 1**.
3) Approve the Redaction Guidance attached at **Appendix 2**.
4) Approve the Vulnerability Disclosure Procedure attached 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)

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 £17 million or 4% of annual turnover (depending on which is larger) for the most serious breaches.

Legal Implications:
(Authorised by the Borough Solicitor)

Robust data and information governance is critical for efficient delivery of services and revenue collection.

In addition non-compliance with the Data Protection Act 2018 and UK GDPR would expose the Council to enforcement action and/or a financial penalty from the Information Commissioners Office which as set out in the financial implications can be significant in addition to the reputational damage to the council.

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 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.

Access to Information:

This report is to be considered in public.

Background Papers:

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

1. INTRODUCTION

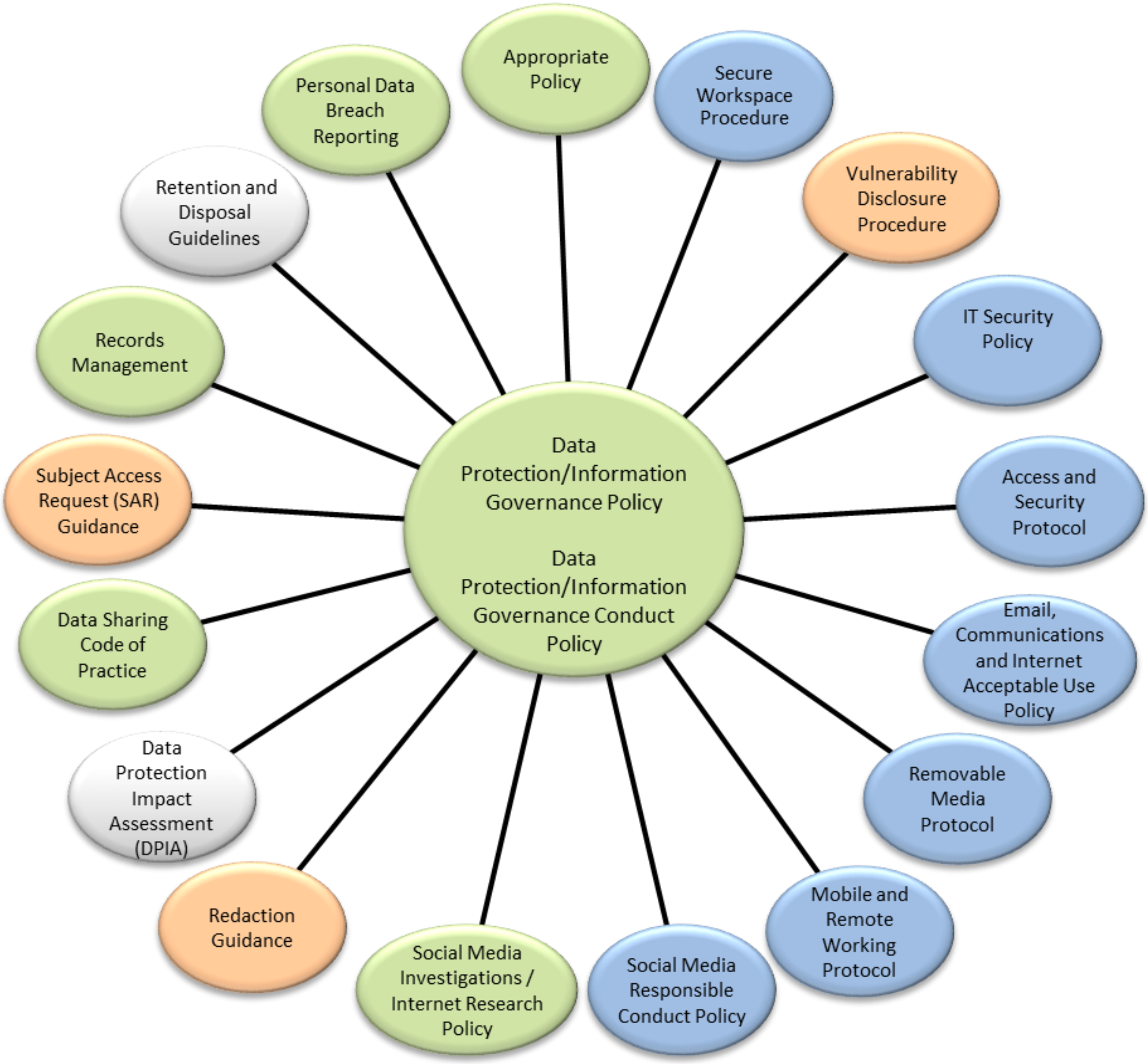
1.1 The primary pieces of legislation relating to information governance and data protection are the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) which came into force from 25 May 2018 and were update to UK GDPR following the UK's departure from Europe.

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 Work Plan for the Information Team is to review the Data Protection/Information Governance Framework, which is presented below. The 'bubbles' are shown in different colours to represent the status of the documents, and the key is detailed in the table at 2.3.

Diagram 1 – Data Protection/Information Governance Framework


Data Protection/Information Governance Policy
Data Protection/Information Governance Conduct Policy
Appropriate Policy
Secure Workspace Procedure
Vulnerability Disclosure Procedure
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
Redaction Guidance
Data Protection Impact Assessment (DPIA)
Data Sharing Code of Practice
Subject Access Request (SAR) Guidance
Records Management
Retention and Disposal Guidelines
Personal Data Breach Reporting

2.3 **Table 1 – Diagram Key**

🟩	Document reviewed, presented and approved by the Audit Panel.
🟦	Review in Process.
🟧	Documents present to below to the Audit Panel.
	Review to commence in Quarter 1 of 2022/23.

3 UPDATED FRAMEWORK DOCUMENTS

3.1 The Information Governance Group, considered three documents at its meeting on 2 December 2021 and these are presented in Appendices 1, 2 and 3 for information. Consultation has taken place with the Information Governance Champions and feedback has been incorporated into the documents attached.

Subject Access Request Guidance

3.2.1 UK GDPR and the Data Protection Act 2018 give individuals various rights, including the right of access to personal information held about them by an organisation, known as a Subject Access Request (SAR). The rights of subject access constitute a statutory duty with strict timescales and any requests must be dealt with promptly and appropriately to ensure compliance with the legislation.

3.3.2 The purpose of this guidance is to set out the various roles and responsibilities within the Council when dealing with a Subject Access Request. The guidance provides the following advice:-

- how to recognise a Subject Access Request,
- the key points to consider and
- the procedure to be followed to ensure fulfilment of the request in line with the data protection legislation

3.2.3 The document attached at **Appendix 1** is an update on the existing policy, which has been refreshed to make the guidance clearer. It updates the SAR process to better reflect the procedures in place within the Information and Improvement Team and wider service areas.

3.2.4 Clarity has been added around how to recognise a SAR and the immediate steps to be taken by any employee to ensure the SAR is dealt with in the right way and in line with statutory timescales.

3.2.5 Redaction guidance has been added to provide further clarity on when and how redaction should be carried out. In responding to a SAR, it is paramount to collate all the related information together and then to review it to ensure only that relating to the data subject is released.

3.2.6 The updated policy covers:

- Introduction;
- Definitions;
- Scope;
- The Right of Subject Access;
- Roles and Responsibilities;
    - Employees;
    - Managers;
    - Heads of Service;
    - Directorate IG Champions
    - Subject Access Request Coordinator (Children's and Adult's Services);
- What makes a Valid SAR Request?
    - Format of request;
    - Asking for clarification;
    - Proof of identity;

    - Requests made on behalf of others;
    - Requests
- Requests for information about Children;
- Handling the SAR;
    - Time limit for complying with a SAR;
    - Process for handling a SAR
    - Format of information being disclosed;
- Requests involving third party personal data;
    - Duty of confident owed to a third party;
    - Other relevant factors;
    - Information about Council Officers;
- Exemptions;
    - Crime and taxation;
    - Health, social work and education;
    - Confidential references;
    - Publicly available information;
    - Negotiations with the requester;
    - Legal professional privilege;
- Complaints about Subject Access;
- Appendix 1 – Redaction Guidance

Redaction Guidance

3.3.1 The document attached at **Appendix 2** is a new guidance document to draw together the current working practices across the Council in respect of redaction, standardise them and provide one central point of reference for all employees to refer to for guidance when faced with a redaction task.

3.3.2 The guidance has been brought in line with current legislative and regulatory guidance. In light of various ICO enforcement actions and reprimands against other organisations in recent years for redaction errors, the procedure regarding how to redact has been refined to ensure that all redaction is carried out electronically using software approved and supplied by IT Services.

3.3.3 As a result of amendments to the guidance, it is considered that further direction and clarity has been provided to the Council's employees and the guidance better underpins the wider Data Protection/Information Governance Framework.

3.3.4 From discussions with both the Information Governance Group and the Information Champions a training course is to be developed to explain not only how to react information using the software but what to redact and why. Officers across the Council with experience and expertise will help to deliver the training.

3.3.4 The guidance covers:

- Introduction;
- Definitions;
- Scope;
- Roles and Responsibilities;
    - Employees;
    - Managers;
    - Heads of Service;
    - Directorate IG Champions
    - IT Services
- What is redaction?; and
- Redaction Principles

Vulnerability Disclosure Procedure

3.4.1 The procedure outlines the process for reporting an external/internal security vulnerability found in any of the Council's hosted systems and/or services to the Council. It sets out expectations of what the reporting individual can expect as part of the reporting process.

3.4.2 The guidance covers:

- Reporting;
- What to Expect;
- Guidance;
  - You Must Not;
  - You Must;
- Legalities; and
- Feedback

4 RECOMMENDATIONS

4.1 As set out on the front of the report.