

Report To:	AUDIT PANEL
Date:	27 July 2021
Reporting Officer:	Kathy Roe – Director of Finance Wendy Poole – Head of Risk Management and Audit Services
Subject:	INFORMATION GOVERNANCE REPORT
Report Summary:	The report provides an update on Information Governance across the Council and presents some key documents for approval.
Recommendations:	<p>Members are asked to:</p> <ol style="list-style-type: none"> 1) Note the report. 2) Approve the Appropriate Policy attached at Appendix 1. 3) Approve the Records Management Policy attached at Appendix 2. 4) Approve the Personal Data Protection Procedure attached at Appendix 3. 5) Approve the Social Media Investigation/Internet Research Policy attached at Appendix 4.
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 Information Governance Framework to enable staff to adhere to the requirement of UK GDPR and the Data Protection Act 2018.
Financial Implications: (Authorised by the statutory Section 151 Officer & Chief Finance Officer)	Non-compliance with the Data Protection Act 2018 or the UK General Data Protection Regulations 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)	Non-compliance with the UK General Data Protection Regulations and the Data Protection Act could expose the Council to an enforcement notice and/or a financial penalty from the Information Commissioners Office.
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 Information Governance Framework is critical if we are to comply with the requirements of the UK GDPR and Data Protection Act.
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

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

2. UK GDPR - SEVEN KEY PRINCIPLES

There are seven principles under UK GDPR as detailed below.

2.1 Lawfulness, fairness and transparency

Personal data should be processed lawfully, fairly and in a transparent manner in relation to individuals.

2.2 Purpose limitation

Personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not to be considered to be incompatible with the initial purposes.

2.3 Data minimisation

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

2.4 Accuracy

Personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

2.5 Storage limitation

Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.

2.6 Integrity and confidentiality (security)

Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2.7 Accountability

Article 5(2) adds that "the controller should be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')." The accountability principle requires organisations to take responsibility for what they do with personal data and how they comply with the other principles. Organisations must have appropriate measures and records in place to be able to demonstrate compliance.

3 COMPLIANCE AT TAMESIDE

3.1 The Council has an Information Governance Framework in place which provides a suite of policies, procedures and guidelines to ensure we are compliant with the requirements of UK

GDPR and the Data Protection Act 2018. The Framework was first introduced in 2013 and a major update was undertaken prior to May 2018.

- 3.2 Information Governance is governed by the Data Protection Officer (DPO) and the Senior Information Risk Owner (SIRO) and the Information Governance Group. The key roles are detailed in Table 1 below:-

Table 1 – Information Governance Key Roles

Role	Officer
Data Protection Officer	Director of Governance and Pensions
Senior Information Risk Owner Information Governance Lead	Head of Risk Management and Audit
Information Governance Team	Risk, Insurance and Information Governance Manager Risk, Insurance and Information Governance Officers Risk, Insurance and Information Governance Assistant
Information Governance Group	DPO SIRO/Information Governance Lead Risk, Insurance and Information Governance Manager Risk, Insurance and Information Governance Officers Assistant Director – Digital Tameside Head of ICT Strategy and Operations Cyber Security Technical Specialist Head of Legal Services/Principal Solicitor Information and Improvement Business Manager Records Manager
Information Governance Champions	Risk, Insurance and Information Governance Manager Risk, Insurance and Information Governance Officers Directorate Representatives Information and Improvement Business Manager Records Manager
Audit Panel	Consider the effectiveness of the authority's risk management arrangements, the control environment and associated anti-fraud and anti-corruption arrangements.
Assistant Directors	Information Asset Owners

- 3.3 Staff need to be trained on a regular basis to ensure compliance with UK GDPR and the Council has met this requirement by mandating training for all staff who use and have access to data and emails. Information governance/data protection training using E-Learning has been rolled out in January 2020 and June 2021 and is detailed below:-

- 2020 – Information Governance and cyber Security
- 2021 – Data Confident and Cyber Ninjas

- 3.4 The existing Information Governance Framework in place is detailed in Diagram 1 below. It is available on the Staff Portal on the Information Governance page which also provides further information and links to guidance. Advice and Support is provided by the Risk, Insurance and Information Governance Team, the Records Manager and the Executive Support Team in terms of Freedom of Information Requests and Subject Access Requests.

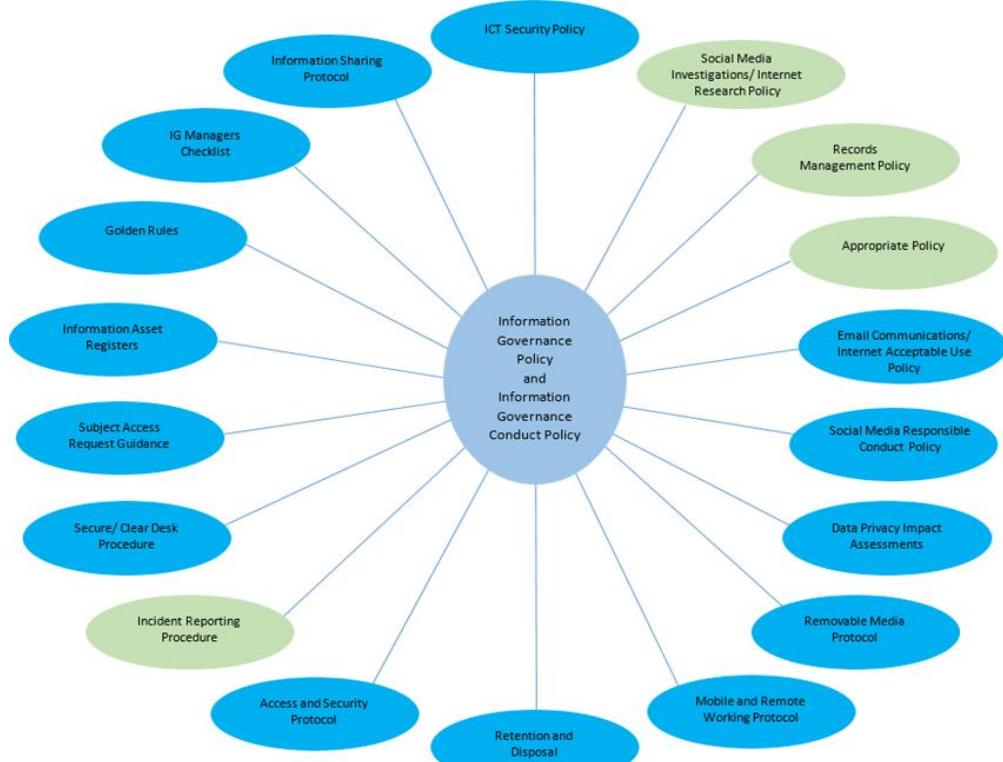
- 3.5 The Council has a public Data Protection page on its website which details:-

- Privacy Notices – providing details of how the Council handles personal data;
- Exercising Your Individual Rights in accordance with UK GDPR; and
- Information Governance Policy

Diagram 1 – Information Governance Framework



Diagram 2 – Revised Information Governance Framework



4

4.1 UPDATING THE FRAMEWORK

The Information Governance Group, chaired by the Data Protection Officer has considered four documents at recent meetings 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 – 4. The updated Information Governance Framework is detailed in Diagram 2 above and the new/updated documents are highlighted in green.

Appropriate Policy

4.2 In order for the Council to carry out its statutory and public functions, the Council processes special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the UK General Data Protection Regulation and Schedule 1 of the Data Protection Act 2018.

- 4.2.1 This policy applies when the Council is processing special category data when relying on the requirements listed in Parts 1, 2 and 3 of Schedule 1 of the Data Protection Act 2018. This policy lists the procedures, which are in place to secure compliance with the UK General Data Protection Regulation and data protection principles, needed when processing special category data.
- 4.2.2 The policy is based on the advice and guidance provided by the Greater Manchester Information Governance Group and is in line with the guidance provided by the ICO and their own document which can be found here - [Policy document – our processing of special categories of personal data and criminal offence data | ICO](#).

The policy is attached at **Appendix 1** and covers:-

- Introduction and Scope
- Policy Statement
- Roles and Responsibilities
- Definition of Special Category Data
- Definition of Criminal Conviction Data
- Policy Document
- Conditions for processing special category and criminal offence data
- Procedures for Ensuring Compliance with the Principles
- Review Date
- Data Protection Officer
- General Enquiries
- Training
- Compliance and Monitoring

Records Management Policy

4.3. The Council appointed a Records Manager in January 2019 to provide structure and guidance in terms of records management, the post sits within the Executive Support Service Unit in the Governance Directorate.

- 4.3.1 Records are a critical asset and are the basis on which decisions are made, services provided and policies developed and communicated. The public has a right to access information under the Freedom of Information Act 2000. These rights are diminished if information cannot be found when requested or, when found, cannot be relied upon as authoritative.
- 4.3.2 Good Records Management will benefit all staff and service areas across the Council and NHS Tameside and Glossop Clinical Commissioning Group (CCG). Benefits include but are not limited to:
- A reduction in time spent searching for information;
 - Improved information integrity due to fewer versions and duplications of documents;
 - Improved transparency and accountability;
 - A reduction in storage costs as data is cleansed;
 - Improved access to information;
 - An open and transparent foundation for decision-making;

- Preservation of the Council's and CCG's corporate memory;
- Supported continuity in the event of a disaster;
- Enhanced customer service and improved reputation with partner organisations;
- Protection and support in litigation;
- Compliance with legislation and regulations such as UK GDPR, the Data Protection Act 1998, employment legislation and health and safety legislation;
- Improved ability to demonstrate corporate responsibilities;
- Business intelligence and analysis of data is reliant on excellent record keeping; and
- Records of value to Tameside are identified and held by the Archive

4.3.3 The Records Management Policy is attached at **Appendix 2** and covers:-

- Introduction
- Scope and Definitions
- Summary of Recommended Good Practice
- Roles, Responsibilities and Expectations of Records Management
- What Records Need to be Kept
- Digital Records Systems
- Scanning Records
- Physical Storage
- Records Shared with and Stored by External Bodies
- Destruction
- Preservation
- Legislation and Related Policies
- Policy Review
- Appendix 1 – Tips for Effective Records Management
- Appendix 2 – IICSA Letter to Chief Executive *
- Appendix 3 – Guidance Note Regarding Retention *
- * Relates to the Independent Inquiry into Child Sexual Abuse (Goddard)
- Appendix 4 – Record Review Form and Questions

Personal Data Breach Reporting Procedure

- 4.4. In order for the Council to demonstrate that it is compliant with UK GDPR it needs a robust breach detection, investigation and internal reporting procedure in place. That will facilitate decision-making about whether a breach needs to be notified to the relevant supervisory authority, the Information Commissioner's Office or the affected individuals, or both.
- 4.4.1 The document attached at **Appendix 3** is an update on the existing procedure, which is currently titled, Information Security Incident Reporting Procedure and Practice Note and it has been refreshed based on experience and feedback received to date. The updated document has been renamed to Personal Data Breach Reporting Procedure as UK GDPR uses that terminology and all reports to the ICO relate to Personal Data Breaches.
- 4.4.2 The reporting form has also been refreshed and the order of the questions has been reviewed and the number condensed to facilitate completion in a timely manner. The deadline of reporting within 24 hours is reiterated within the document to enable the Council to meet its obligation of reporting within 72 hours of becoming aware of a breach. An E-Form has also been designed by ICT Services to provide an accessible tool to encourage managers to report all potential breaches within the 24 deadline.
- 4.4.3 The procedure consists of the following sections:-
- Introduction
 - Definitions
 - Roles and Responsibilities
 - Reporting a Potential Personal Data Breach
 - Breach / Near Miss Investigation
 - Initial Response

- Investigation Process
- Evaluation
 - Assessment of Ongoing Risk
- Action / Outcomes
 - Notification
 - Disciplinary Action
 - Policy and Procedural Changes
 - Employee Notification and Training
- Appendix 1 – Categories/Examples of Breaches and Near Misses
- Appendix 2 – Personal Data Breach Reporting Form (PDBRF01)

4.4.4 Appendix 1 in the updated procedure provides a list of:-

- Types of Potential Breach (based on experience)
- What Does a Breach look like?
- What does a Near Miss look like?

Social Media Investigations/Internet Research Policy

4.5. It is recognised that the use of the internet and, in particular, social networking sites, can provide useful information for council staff carrying out research and/or investigations. These investigations may relate to the various organisational roles within the Council – for example, Fraud, Planning Enforcement, Education, Exchequer, Licensing, Environmental Health, but will equally apply to some non-enforcement teams, such as Adult Social Care.

4.5.1 The use of the internet and social networking sites may potentially fall within the definition of covert directed surveillance. This is likely to result in the breaching of an individual's Article 8 rights under the Human Rights Act (right to privacy). This use of online open source internet and social media research techniques will be a productive method to assist the Council with its regulatory and enforcement functions. It can also assist with other functions such as service delivery issues and debt recovery.

4.5.2 However, the use of the internet and social media is constantly evolving and with it the risks, particularly regarding breaches of privacy. So researching, recording, storing and using open source information regarding a person or group of people must be necessary and proportionate to protect the Council.

4.5.3 This policy sets out the framework on which the Council may utilise Social Media when conducting research and/or investigations. The aim of this policy is to ensure that investigations and/or research involving the use of Social Media are done so lawfully and correctly. The policy establishes the Council's corporate standards and instructions, which will ensure that all online research and investigations are conducted lawfully and ethically to reduce risk. It provides guidance to all staff, when they are engaged in their official capacity of the implications and legislative/best practice framework associated with online internet and social media research. It will also ensure that the activity undertaken, and any evidence obtained will stand scrutiny.

4.5.4 The aim is to ensure that information gathering, investigations or surveillance involving the use of Social Media are conducted lawfully and correctly in accordance with an individual's human rights and with due consideration of relevant legislation including:

- Human Rights Act 1988 (HRA)
- European Convention on Human Rights (ECHR)
- Data Protection Legislation (Data Protection Act 2018 (DPA))
- Regulation of Investigatory Powers Act 2000 (RIPA) together with the published codes of practice from the Home Office, Investigatory Powers Commissioner's Office (IPCO), formerly the Office of Surveillance Commissioners (OSC), and the Information Commissioner's Office

4.5.5 The policy attached at **Appendix 4** covers:-

- Background of Policy
- Legal Framework
- What is Meant by Social Media
- Utilising Social Media Within an Investigation
- Privacy Settings
- Risk
- Necessity/Justification
- Proportionality
- Private Information
- Collateral Intrusion
- Covert Human Intelligence Source (Chis)
- Definition of a Chis
- What is Permitted Under This Policy
- Council Policy Reflected across Directorates
- Teams within Regulatory Services
- Children and Families
- Adult Health and Social Care
- One-Off Visits
- What is not Permitted under this Policy
- Use of Official Organisation
- Departmental Social Media Accounts
- Capturing Evidence
- Activities by Members of The Public
- Use of Information and Material Obtained
- Preservation of Evidence
- Written Activity Records
- Reviewing the Activity

4.5.6 Once approved, implementation of the policy needs to be determined, so that controlled access is granted to a dedicated Social Media Account for the specific purpose of gathering information for investigations and ensuring investigators are acting lawfully. Online investigation tools are being reviewed.

4.5.7 Investigators will be required to attend training and options for delivery are being reviewed. If the potential expenditure in relation to the training and 4.5.8 above exceeds available budgets a funding bid will be prepared and submitted for consideration.

5 RECOMMENDATIONS

5.1 As set out on the front of the report.