Report To:	**AUDIT PANEL**
Date:	29 May 2018
Cabinet Deputy/Reporting Officer:	Wendy Poole - Head of Risk Management and Audit Services
Subject:	**INFORMATION GOVERNANCE**
Report Summary:	To provide an update on the requirements of the General Data Protection Regulations (GDPR) and the new Data Protection Act.
Recommendations:	1. Members note the report. 2. Members approve the Information Governance Framework documents attached at **Appendices 1 – 12**.
Links to Community Strategy:	Strong information governance supports the individual operations, which deliver the objectives of the Council.
Policy Implications:	Data Protection legislation is changing from May 2018. The Data Protection Act 1998 will be replaced by the General Data Protection Regulations which become effect from 25 May 2018 and a new Data Protection Act. It is therefore critical that policies and procedures are updated to ensure compliance with the new regulations/act.
Financial Implications: (Authorised by the Section 151 Officer)	Non-compliance with the Data Protection Act 2018 or the General Data Protection Regulations can result in the Information Commissioner's Office imposing financial penalties up to maximum of €20 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 General Data Protection Regulations and the new 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 and commit the necessary resources within service areas to support the corporate Risk and Insurance Team will be critical if we are to comply with the new requirements of the GDPR and Data Protection Act.

Access to Information:

Background papers can be obtained from the author of the report, Wendy Poole, Head of Risk Management and Audit Services by contacting:

Telephone:0161 342 3846

e-mail: wendy.poole@tameside.gov.uk

1. INTRODUCTION

1.1 Significant changes are happening in relation to Data Protection legislation in May 2018.

1.2 The General Data Protection Regulations (GDPR) come into operation from 25 May 2018 and will effectively replace the current EU derived rules enshrined in the Data Protection Act 1998.

1.3 The Data Protection Bill which is currently progressing through the House of Lords contains a number of inter-related objectives and it is envisages that it will be enacted in May 2018.

1.4 It is important to note that GDPR is an evolution in data protection and not a revolution. It demands more on organisations in terms of accountability for their use of personal data and enhances the existing rights of individuals. It builds on the foundations already in place for the last 20 years.

1.5 Many of the fundamentals remain the same and have been known about for a long time; fairness, transparency, accuracy, security, minimisation and respect for the right of the individual. The General Data Protection Regulations strengthens the controls that organisations (data controllers) are required to have in place over the processing of personal data.

1.6 The Information Commissioners Office has produced a guidance document entitled "12 Steps to Take Now" which can be found here, which explains where there is continuity, what's new and how to plan. This together with the regulations has been used to inform the work plan for the Council which is monitored by the Information Governance Group. As we have an established Information Governance Framework in place, we are developing systems and processes already in place.

2 PURPOSE OF THE REPORT

2.1 To provide the Audit Panel with an overview of the work that is ongoing to ensure that the Council has a plan of action in place to move towards full compliance with both the General Data Protection Regulations and the new Data Protection Act 2018.

2.2 Whilst 25 May 2018 is quoted as being the date for the General Data Protection Regulations to become effective, the Information Commissioner has clearly stated that 25 May is the beginning of a journey and not the end.

2.3 Work has concentrated on the following areas:-

- Creating information asset registers for all service areas, by facilitating workshops with managers to collate data in a template approved by the AGMA Information Governance Group;
- Using those registers, to create privacy notices for publication on the public website;
- Producing a Record of Processing Activities (ROPA) which will need to be published on our website and this will be based on the information asset registers from service areas;
- Reviewing the Information Governance Framework documents in line with the new requirements;
- Identifying the best training and communications methods to ensure messages and training reach all staff in the most useable and appropriate way;
- Producing a Contract Variation letter to be sent to all contractors, suppliers and processors; and
- The introduction of an Information Governance Newsletter.

3 KEY CHANGES

3.1 Down from 8 principles to 6. These are:

- Personal data (anything information that can identify a living individual) must be processed fairly, lawfully, and in a transparent manner;
- Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible;
- Adequate, relevant and limited to what is necessary;
- Accurate and where necessary kept up to date;
- Kept in a form that permits identification of the data subject for no longer than is necessary; and
- Processed in a manner that ensures appropriate security.

3.2 Breaches of personal data that result in a risk to the rights and freedoms of individuals must generally be reported to the ICO within **72 hours**.

3.3 Under GPDR, fines can be issued for security breaches and where an organisation cannot demonstrate compliance with any of the Principles. Fines increase up to €20million or 4% of annual turnover (depending on which is larger).

3.4 The council must be able to demonstrate that we are compliant with the GDPR, i.e. having appropriate policies and procedures in place for the governance of all personal data processed. This includes keeping a record of:

- what types of information we process;
- why we process the information;
- who the information is about;
- who we share the information with;
- a general description of our security measures;
- our retention policy and schedule; and
- any transfers to third countries outside of the EU.

3.5 Sensitive personal data becomes ‘special categories’ of data.

3.6 Consent is a much higher standard. It must be opt-in and clear, explicit and freely given and demonstrable, preferably time limited, and given to the data subject in an age appropriate, plain language format. The data subject must also be informed that they are able to withdraw their consent at any time as easily as it is given.

3.7 A Data Protection Officer (DPO) must be appointed.

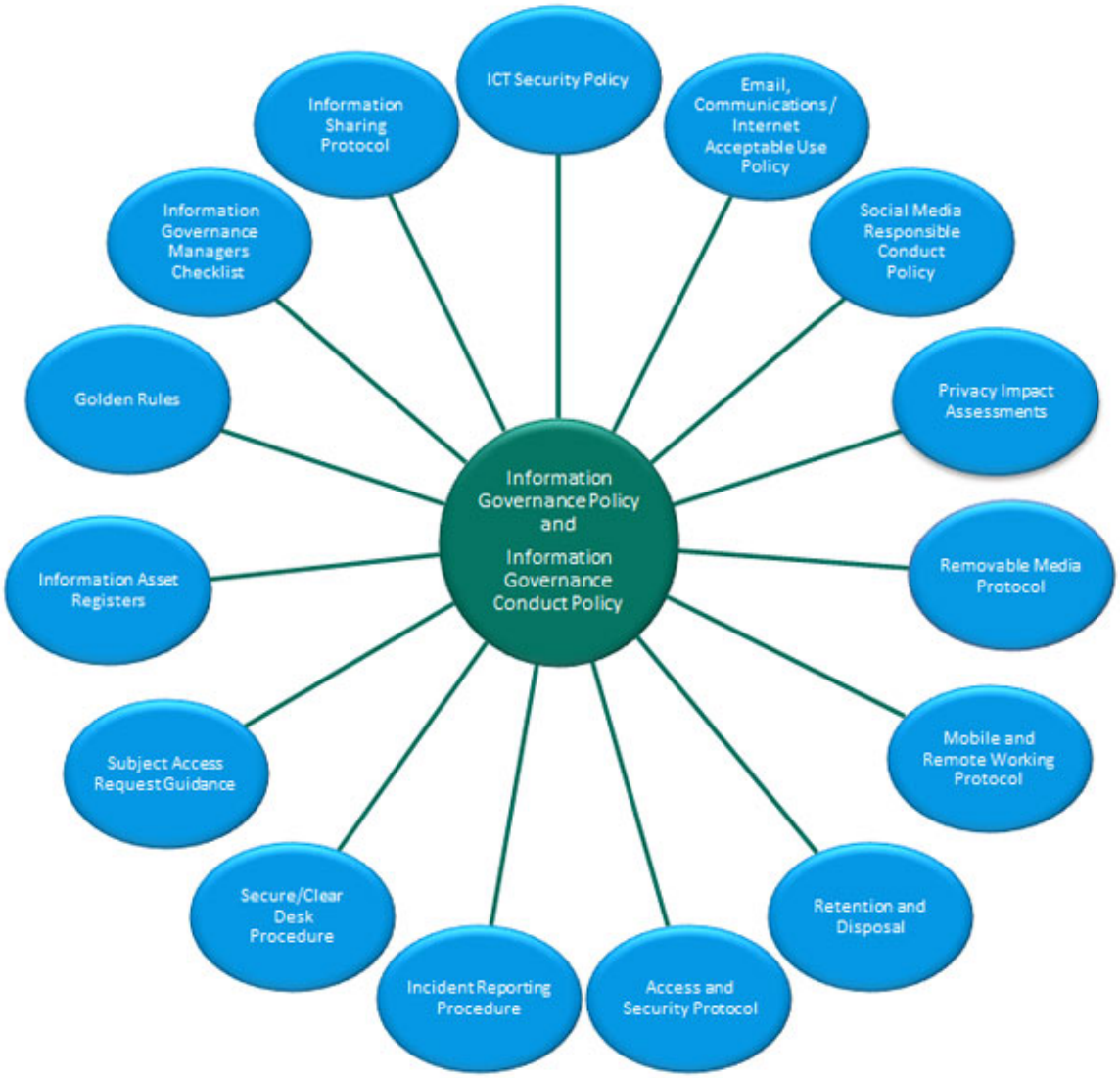
3.8 Subject Access Rights (SARs) are still the cornerstone of the GDPR. However, individuals also have new rights under the GDPR, these new rights include:

- The right to erasure/to be forgotten;
- The right to object;
- The right to data portability;
- The right to rectification;
- The right to restrict processing;
- Subject Access Request response time is now 1 month (previously 40 days), this can be extended by a further 2 months if the request is highly complex or large in volume; and
- The £10 fee is removed.

4 INFORMATION GOVERNANCE FRAMEWORK

4.1 The Information Governance Framework was introduced in 2013 and has been updated since then as new guidance and advice has been received and published by the Information Commissioners Office. The current framework is shown in the diagram below.

4.2 Diagram 1 – Information Governance Framework



4.3 The documents detailed in the table 1 below have been refreshed and updated in light of the General Data Protection Regulations (GDPR).

Table 1 – Information Governance Framework Review

Document Title	Last Updated	GDPR ready? (Y/N)	Appendix No.	Comments
Information Governance Policy	Nov 2016	N	1	The overarching documents have been refreshed and updated to reflect changes made in the supporting documents and to reflect changes to legislation.
Information Governance Conduct Policy	Nov 2016	N	2	
ICT Security Policy	Nov 2013	Y	3	Refreshed and updated to reflect changes to legislation.

Document Title	Last Updated	GDPR ready? (Y/N)	Appendix No.	Comments
Email, Communications and Internet Acceptable Use	Nov 2013	Y	4	Refreshed and updated to reflect changes to legislation.
Social Media Responsible Conduct	Nov 2013	Y	5	This was approved by the Standards Committee in October 2017 and slightly amended now to remove reference to the Data Protection Policy and replace with the Information Governance Framework.
Removable Media Protocol	Nov 2013	Y	6	Refreshed and updated to reflect changes to legislation and definitions.
Mobile and Remote Working Protocol	Nov 2013	Y	7	Refreshed and updated to reflect changes to legislation and definitions.
Access and Security Protocol	Nov 2013	N	8	Refreshed and updated to reflect changes to legislation.
Information Security Incident Reporting Procedure	Nov 2016)	N	9	This document has been refreshed and reviewed to reflect the new requirement to notify the ICO with 72 hours of a notifiable breach.
Secure/Clear Desk Procedure	Nov 2013	Y	10	Refreshed and updated to reflect changes to legislation
Golden Rules	Nov 2013	Y	11	Refreshed and updated to reflect changes made to other documents.
Subject Access Request Guidance	Nov 2016	N	12	The guidance has been updated to reflect that the timescales for responding has reduced from 40 days to 1 month. The fee of £10 has been removed. Extensions will only be granted in exceptional circumstances and the age of consent has been lowered to 13. Information requested needs to be manageable/useable and easy to understand.

4.4 The documents detailed in the table 2 below have not been refreshed and updated yet as more work needs to be undertaken in light of the Information Asset audits undertaken.

Table 2 – Information Governance Framework Documents to be reviewed

Document Title	Last Updated	Comments
Retention and Disposal Schedule	Nov 2013	This will be reviewed once the information audits have been completed so that the existing schedule can tailored to the Council.
Managers Checklist	Nov 2013	This will need to be reviewed to reflect changes made to all other documents.
Information Sharing	Nov 2013	Use of consent and privacy notices need to be reviewed, together with individual's rights.

Document Title	Last Updated	Comments
Protocol		Processors will have the same responsibilities as owners.
Data Protection Impact Assessments	New Requirement	The document produced by the Information Commissioner's Office is being reviewed.

5 TRAINING AND AWARENESS

5.1 Discussions with People and Workforce Development have commenced to ensure that training and awareness is targeted at the right people in a format that meets their needs. A new Mandatory E-Tutorial - General Data Protection Regulations has been rolled out for completion by the end of June.

5.2 Consideration is also being given to delivering some Manager Briefings about the key changes in relation to Subject Access Requests, Reporting Information Incidents and dealing with the new rights for Individuals.

5.3 Articles have been published in Live Wire and in the Chief Executive's Brief.

6 RECOMMENDATIONS

6.1 Members note the report.

6.2 Members approve the Information Governance Framework documents attached at **Appendices 1 – 12.**