STAFFORDSHIRE MOORLANDS DISTRICT COUNCIL

Report to Cabinet

13 February 2018

TITLE:	**Information Governance Framework**
PORTFOLIO HOLDER:	**Councillor Tony Hall – Customer Services**
CONTACT OFFICER:	**Executive Director (People) and Monitoring Officer**
WARDS INVOLVED:	**All**

Appendices Attached

Appendix A – GDPR Action Plan
Appendix B – Information Governance Policy

1. Reason for the Report

The Council must comply with a number of different Acts and Regulations when processing information. Failure to process information properly can lead to a range of problems including poor decision making, inefficient business processes, inconvenience or harm to residents and others, reputational damage to the Authority, and/or enforcement action by the Information Commissioner's Office. Enforcement action can include fines of up to £500,000 for serious breaches of the Data Protection Act 1998 and possible prison sentences for deliberate breaches.

This report introduces an information governance framework for managing information and the associated risks, and supporting regulatory, legal, and operational requirements.

2. Recommendation

2.1 That the Cabinet notes the content of the report and approves the proposed approach to information governance.

2.2 That the Council will register all Councillors with the ICO, and meet the registration costs, unless individual councillors wish to opt-out from registering.

3. Executive Summary

3.1 Information is an important council asset and an essential element in the provision, and effective management, of quality services for our local communities. Council information includes internal information, external information, strategic information and council information held within the supply chain.

3.2 Information governance (IG) is a set of multi-disciplinary structures, policies, procedures, processes and controls that are implemented to manage information at an organisational level, and designed to support regulatory, legal, risk, environmental and operational requirements. It encompasses areas such as records management, IT and information security, data handling, data protection, risk management, data storage, archiving and data disposal. The Alliance approach to information governance – ASSURED- has been designed to reflect the lifecycle of information: source (obtain) data, store, use (or share), retain, and erase (or dispose) when the data is no longer required.

3.3 Appendix A presents a proposed Information Governance Policy. The Council will also develop and maintain a number of local policies and guidance to support this overarching information governance policy, which together will provide an information governance framework. These documents will include a:

- Data Protection Policy;
- Protective Marking, Handling and Disposal Policy;
- Information Handling guidance;
- Document Retention Policy; and
- IT and Information Security Policy.

3.4 The report also provides an update regarding the requirement for councillors to be registered on an individual basis under the Data Protection Act 1998 and proposes that the Council ensures registration with the ICO for all councillors.

4. How this report links to Corporate Priorities

4.1 The information governance policy will assist the Council to use information appropriately to deliver its corporate priorities.

5. Options and Analysis

5.1 Cabinet approves the outlined approach to Information Governance (recommended).

5.2 Cabinet does not approve the outlined approach (not recommended).

6. Implications

6.1 Community Safety - (Crime and Disorder Act 1998)

There are no specific implications.

6.2 Workforce

All Council employees will be expected to comply with the information governance framework.

6.3 Equality and Diversity/Equality Impact Assessment

There are no specific implications. Individual services will, however, be required to consider the impact on individuals when processing information.

6.4 Financial Considerations

None – any costs will be met from within existing service budgets.

6.5 Legal

There are a number of legal and other obligations placed upon the Council when processing information, including the Data Protection Act 1998; the Human Rights Act 1998, Freedom of Information Act 2000, and Environmental Information. The policy will assist the Council to meet such obligations.

6.6 Sustainability

Not applicable.

6.7 Internal and External Consultation

None.

6.8 Risk Assessment

The policy will assist the Authority to manage the risks associated with the processing and other handling of information.

7. Background and Detail

7.1 Information is an important council asset and an essential element in the provision, and effective management, of quality services for our local communities.

7.2 Council information includes internal information (e.g. HR data, finance data), external information (e.g. information about residents, businesses), strategic information (strategic planning, transformation plans) and council information held within the supply chain (e.g. suppliers, cloud computing).

7.3 Information governance (IG) is a set of multi-disciplinary structures, policies, procedures, processes and controls that are implemented to manage information at an organisational level, and designed to support regulatory, legal, risk, environmental and operational requirements. It encompasses areas such as records management, IT and information security, data handling, data protection, risk management, data storage, archiving and data disposal.

7.4 The Alliance approach to information governance – ASSURED- has been designed to reflect the lifecycle of information: source (obtain) data, store, use (or share), retain, and erase (or dispose) when the data is no longer required (Figure 1).

7.5 An information governance policy has been developed to provide a framework that ensures that the Council:

- recognise, and treat, information as a valuable asset;
- recognise the cost involved in the creation, storage and other processing of information and the need to do so in a cost-effective manner;
- recognise the risk to the Council of information breaches in terms of financial loss, reputational harm and/or disruption to service delivery;
- comply with relevant legislation, for example the Data Protection Act 1998 and Freedom of Information Act 2000;
- have in place policies, procedures and guidelines to support appropriate information handling and management;
- demonstrate organisational commitment by setting out roles and responsibilities of staff members; and
- have in place appropriately trained staff members to ensure compliance with the framework.

7.6 The Council will also develop and maintain a number of local policies and guidance to support this overarching information governance

policy, which together will provide the Alliance's information governance framework. These documents will include a:

- Data Protection Policy;
- Protective Marking, Handling and Disposal Policy;
- Information Handling guidance;
- Document Retention Policy; and
- IT and Information Security Policy.

7.7 The Executive Director (People) and Monitoring Officer will act as Senior Information Risk Officer (SIRO) with overall responsibility for overseeing the Council response to information risk. The SIRO chairs a quarterly Information Governance Group attended by the owners of the Council's information assets (e.g. CCTV, Council Tax, Housing, Revenues and Benefits systems, etc) to promote good practice, highlight non-compliance, identify possible risks and take steps to mitigate against such risks. The Council will use the acronym ASSURED (above) to promote awareness and compliance of the information governance framework.

General Data Protection Regulation

7.8 The Data Protection Act (DPA) 1998 transposed the EU Data Protection Directive 95/46/EC into UK law. The EU's data protection framework has been revised and a new General Data Protection Regulation[1] ("the GDPR") comes into force on 25th May 2018.

7.9 The GDPR will no longer have effect once the UK leaves the EU but a new Data Protection Bill is currently being considered by Parliament. The Bill transposes the GDPR into UK law and also provides detail on the derogations available under the GDPR (notably rights of children, processing of information about criminal convictions and offences, and exemptions).

7.10 Many of the GDPR's requirements are similar to those in the current Data Protection Act but changes include:

- Increased territorial scope (the GDPR applies to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location).
- Increased penalties (organisations can be fined up to 4% of annual global turnover or €20 Million (whichever is greater) for a breach of requirements).
- Strengthened conditions for consent.
- Mandatory notification of breaches where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach.

[1] Regulation (EU) 2016/679

- The right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose.
- The right for an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing (right to erasure or 'right to be forgotten').
- The right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller (data portability).
- Privacy by design.
- Expanded role for data protection officers.

7.11 The Council has developed an action plan for responding to the introduction of the GDPR. This is based upon the Information Commissioner's guide on preparing for the GDPR. A copy of this action plan is provided at Appendix A and the implementation of the plan will be monitored by the internal Information Governance Group. A further report will be provided for Councillors after the GDPR has come into effect.

Update on Requirement for Individual Councillors to be registered under the Data Protection Act 1998

7.12 The Council has obtained the opinion of the Information Commissioner's Office on registration by individual councillors. The ICO have confirmed that when a councillor is carrying out the local authority's functions, such as sitting on a council committee, then they do not need to register in their own right and will be covered by the council's data protection registration.

7.13 ICO guidance also advises that councillors are entitled to rely upon the registration of their political party when acting on behalf of that party, such as campaigning to be a ward councillor. If a prospective councillor is not part of any political party but campaigning to be an independent councillor for a particular ward then they need to have their own registration.

7.14 The ICO have, however, also stated that, "It is our opinion that elected councillors who process personal data electronically for the purpose of constituency casework will be required to have their own registration". Although it is considered by officers that such casework is carried out as part of a councillor's role as member of the local authority and thus would be covered by the council's data protection registration, we feel obliged to recommend that all Councillors follow the advice provided by the ICO and register individually. It is proposed that the Council will register and meet the registration costs for all Councillors. If any councillor does not wish to be registered, for example because they are already registered because of their role as a County Councillor, then they are asked to contact Member Services to opt-out.

7.15 The requirement to notify the ICO in the same way will not continue under the GDPR. However, a provision in the Digital Economy Act means that it will remain a legal requirement for data controllers to pay the ICO a data protection fee. A three tier system is proposed that differentiates between small and big organisations and how much personal data an organisation is processing. It is likely that the Council will be required to pay an annual fee of either £55 or £80 per year. The lower figure would also presumably apply to registration by individual councillors. The final fees are yet to be approved by Parliament and the new approach in due to commence on 1 April 2018.

Mark Trillo
Executive Director (People) and Monitoring Officer

Background Papers	**Location**	**Contact details**
Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now.	https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf	David Smith x 4165

Appendix A: GDPR Action Plan

Steps	ICO Guidance	Key changes	Implications for the Council	Actions
Awareness	You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.	Not applicable.	Requires awareness raising amongst staff and elected members. This should include awareness of changes and training on implementing.	Produce report for Councillors. Article in Keeping You Informed. Training.
Council information	You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.	The GDPR requires the Council to maintain records of its processing activities.	The Councils do not currently have a central register of the personal information that they hold.	Complete information audits. Records need to be maintained and updated.
Communicating privacy information	You should review your current privacy notices[2] and put a plan in place for making any necessary changes in time for GDPR implementation.	The GDR requires some additional information to be included in privacy notices	Councils need to review their current use of privacy notices	Review current privacy notices and update as necessary. Council privacy notice on website has been updated.
Individuals' rights	You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.	On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. The right to data portability is new	Council systems need to be able to both delete personal information and export in usable electronic format.	Service areas need to consider how they would delete personal data if required to and also how they would provide data in an electronic format.
Subject access requests	You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information	• In most cases, the Council will not be able to charge for complying with a request The timescale for responding to requests is reduced from 40 days to a month • The Council can refuse or	The Councils need to update their procedures for responding to Subject Access Requests and, in particular, streamline processes to allow compliance within the reduced timescales.	Introduce Infreemation to manage Subject Access Requests. System has been commissioned and is currently being tested. Update procedure. Train employees.

[2] The Council is required to give people certain information, such as how it intends to use their information, when collecting personal data. This is usually done through a privacy notice.

Steps	ICO Guidance	Key changes	Implications for the Council	Actions
		charge for requests that are manifestly unfounded or excessive. • If applications are refused then individuals must be informed that they have the right to complain to the ICO and to a judicial remedy.		
Lawful basis for processing personal data	You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.	Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data.	The Councils do not currently routines the basis on which personal data is being processed. This increases the possibility of unlawful processing of data.	Individual services need to carry out a review of the personal data that they process and then either document the lawful basis for processing such data or stop processing. This links to the review of privacy notices.
Consent	You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.	The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action. You will need clear and more granular opt-in methods, good records of consent, and simple easy-to-access ways for people to withdraw consent.	The Councils need to be clear that consent is being clearly obtained, and recorded, where required.	All services need to review their forms and ensure that consent is being clearly obtained where necessary.
Children	You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity	The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you	The Council does not generally offer online services to children and collects their personal data. Some events involving schools and/or young people are	Consent forms need to be reviewed and potentially revised for any activity involving the collection of young people's data.

Steps	ICO Guidance	Key changes	Implications for the Council	Actions
		will need to get consent from a person holding 'parental responsibility'.	organised by the Council.	
Data breaches	You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.	The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals.	System already in place.	Promote current system. Monitor breaches at quarterly Information Governance meetings.
Data Protection by Design and Data Protection Impact Assessments	You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.	The GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.	The Councils have already developed an approach to Privacy Impact Assessments, which is compliant with the GDPR requirements.	None
Data Protection Officers	You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.	Public authorities are required to designate a Data Protection Officer. Guidelines on DPOs have been produced by the Article 29 Data Protection Working Party.	Council must confirm designated Data Protection Officer.	The GDPR does not restrict DPOs from holding other posts but expressly requires that controllers and processor ensure that such other tasks do not give rise to a conflict of interest for the DPO. The Councils must consider conflicts of interest.
International	If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.	Not applicable to the Council.	Key Council areas are elections (overseas voters) and Regulatory Services (export licences).	Systems already in place for elections. Review process for export licences.

Steps	ICO Guidance	Key changes	Implications for the Council	Actions
Contracts	Not applicable	Article 28 of the GDPR adds a requirement upon controllers (the organisation who determines the purposes and manner in which personal data is processed) to ensure that certain provisions are included in contracts where there is personal data being passed from one party as the controller of that data to another acting as a processor of that personal data	All new contracts must include certain information prescribed by Article 28.	Standard procurement terms and contract management arrangements need to be updated.