INFORMATION GOVERNANCE POLICY

1. Introduction

The Alliance (High Peak Borough Council and Staffordshire Moorlands District Council) recognises that information is an important asset and an essential element in the provision, and effective management, of quality services for our local communities. Council information will include 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).

The aim of this policy is to provide an information governance framework that ensures that the two Councils:

- 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.

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.

2. Legislative Requirements

There are a number of legal and other obligations placed upon the two Councils when processing information which will inform the way information governance is applied. These include:

- The Data Protection Act 1998 (as amended by the Data Protection Bill and provisions of the General Data Protection Regulation);

- The Human Rights Act 1998
- Freedom of Information Act 2000;
- Privacy and Electronic Communications Regulations
- Regulation of Investigatory Powers Act 2000
- Misuse of Computers Act 1990
- Environmental Information Regulations
- Local Government Act 1972;
- The Public Services Network Code of Connectivity;

3.   Our Approach

The Alliance approach to information governance – ASSURED- has been designed to reflect the lifecycle of information (Figure 1).

Figure 1   ASSURED: the information lifecycle

Our approach:

Information Life Stage	The Council will
Source data	- obtain information fairly and lawfully. - record information accurately and reliably. - take reasonable steps to ensure that any information held is accurate and up-to-date.
Store	- hold information securely to reduce the risk of accidental loss of data, physical system failures (infrastructures failures and breaches) and direct malicious cyber-attacks. - develop systems and processes to allow efficient and effective use of information to assist in the delivery of quality services. - ensure the security of information where it is transferred between services or physical location.
Use/Share	use information to support the targeted delivery of quality services.

	• only use data fairly and lawfully. • be transparent about how we use data. • share information appropriately and legitimately.
Retain	• archive information, where appropriate, to make efficient use of IT, office space and other resources. • retain information in line with data protection and other legislative requirements • make sure that data is not kept longer than is necessary for the purpose that it was collected
Erase	• appropriately dispose of information in a secure and timely fashion.

The Councils 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.

4. Roles and Responsibilities

To support the effective delivery of the information governance policy, the Alliance will:

- Appoint a member of the Senior Management Team to act as Senior Information Risk Officer (SIRO) with overall responsibility for overseeing the Council's response to information risk;
- Appoint a Data Protection Officer to ensure compliance with the Data Protection Act;
- Appoint a lead officer to ensure compliance with the Freedom of Information Act;
- Establish an 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 identify possible risks and take steps to mitigate against such risks;
- Require all managers to take responsibility for ensuring that the requirements of the IG framework are integrated into service procedures, including risk registers, and that staff comply with the framework in their area of responsibility.
- Require all persons to which this policy applies to process information in line with the IG framework. This includes complying with individual policy requirements and undertaking mandatory IG training as required.

5.   Awareness, Training and Compliance

The Alliance will take steps to raise awareness of the information governance framework, including through the induction process for new staff members, regular internal briefings and the Plan, Enable, Perform (PEP) appraisal process. This will be based around the ASSURED mnemonic, which has been developed to reflect the information lifecycle (above).

Training is at the core of Information Governance and will be delivered in a targeted way using a variety of different formats.

All employees have a contractual responsibility to be aware of and conform to the Council's values, rules, policies and procedures. Breaches of policy may lead to the employee going through the relevant Council's disciplinary procedure in accordance with the Code of Conduct and the disciplinary policy and procedure.

Individuals who are not Council employees and who fail to comply with the Councils' policies may have their access to Council information and ICT revoked and such action could have an impact on contracts with third party organisations.