Agenda Item No 8(b)

North East Derbyshire District Council

Cabinet

11 June 2014

Information Management Strategy

Report No: PW/05/14/JF of Councillor P Williams, Portfolio Holder with Responsibility for Information Technology, E-Information and Asset Management

This report is public

Purpose of the Report

- To seek Cabinet approval on the new Information Management Strategy
- To meet legal requirements.

1 Report Details

1.1 This joint strategy sets out the ambitions of both Bolsover District Council and North East Derbyshire District Council in the area of information management. Both councils recognise the importance of information to the daily work of the authorities.

1.2 The strategy has been produced to ensure that both Councils manage information in line with guidance set out nationally.

1.3 The strategy is largely an internal document which sets out what we need to do over the coming 3 years to ensure compliance.

1.4 The strategy has a number of actions identified which have been incorporated into an action plan. This will be monitored and reported on the Councils performance management system.

2 Conclusions and Reasons for Recommendation

2.1 The strategy meets a number of external drivers and compliance requirements including the Public Service Network (PSN) compliance. As such it is essential that a strategy is put in place as a matter of urgency.

3 Consultation and Equality Impact

3.1 The strategy has been developed with a number of officers in Customer Service and Improvement and ICT, to ensure that it is fit for purpose. The strategy has been approved by SAMT and SAJC for submission to members for approval.

3.2 External consultation and an Equality Impact Assessment are not necessary as the actions are largely internal, are that of legal compliance and do not have a direct impact on any group of customers or employees.

4 Alternative Options and Reasons for Rejection

4.1 In preparing the strategy consideration has been given to how best the required actions can be achieved within limited resources.

5 Implications

5.1 Finance and Risk Implications

5.1.1 The strategy allows us to deal with a potential risk of none compliance. Without an agreed way forward, services supported by Government systems could be withdrawn resulting in both Councils being unable to deliver key services to the public.

5.1.2 Financial penalties could be imposed by the Information Commissioners Office (ICO) if Data Protection legislation is breached.

5.1.3 The costs identified for Baseline Personal Security Standard (BPSS) checks (which are mandatory currently) have been agreed at SAMT.

5.2 Legal Implications including Data Protection

5.2.1 The strategy allows compliance with both the Public Service Network (PSN) requirements and the Payment Cards Industry (PCI-DSS) requirements. It is also in line with the requirements of the Data Protection Act and other legislation as detailed in the strategy.

5.3 Human Resources Implications

5.3.1 The strategy details training and development implications.

6 Recommendation

6.1 That Cabinet note the requirement for the (Joint) Information Management Strategy and approve the strategy.

6.2 That the (joint) Information Management Strategy be published on the intranet and internet once approved by Cabinet at North East Derbyshire District Council.

7 Decision Information

Is the decision a Key Decision? (A Key Decision is one which results in income or expenditure to the Council of £50,000 or more or which has a significant impact on two or more District wards)	No
District Wards Affected	All Wards
Links to Corporate Plan priorities or Policy Framework	High Performing Council - NEDDC

8 Document Information

Appendix No	**Title**
A	Information Management Strategy
Background Papers (These are unpublished works which have been relied on to a material extent when preparing the report. They must be listed in the section below. If the report is going to Cabinet (NEDDC) or Executive (BDC) you must provide copies of the background papers)	
As detailed in the strategy	

Report Author	**Contact Number**
Jane Foley, Joint Assistant Director – Customer Service and Improvement	NEDDC - 7029

AGIN 8(b)(CAB 0611) Information Management Strategy/AJD

Appendix A

(Joint) Information Management Strategy 2014-2017

April 2014

CONTROL SHEET FOR: (Joint) Information Management Strategy

Strategy Details	Comments / Confirmation
	(Joint) Information Management Strategy 2014- 2017
Current status – i.e. first draft, version 2 or final version	Final- April 2014
Strategy author	Joint Assistant Director- Customer Service and Improvement
Location of strategy i.e. L-drive, shared Drive	
Member route for approval	Strategic Alliance Joint Committee Executive (BDC)/ Cabinet (NEDDC)
Cabinet Member (if applicable)	
Risk Assessment completed (if applicable)	Risk considered within the strategy
Equality Impact Assessment approval date	Internal document with no direct impact on customers or community groups.
Partnership involvement (if applicable)	Not applicable
Final strategy approval route i.e. Executive/ Council /Planning Committee	Executive (BDC)/ Cabinet (NEDDC)
Date strategy approved	
Date strategy due for review (maximum three years)	April 2017

Date strategy forwarded to Customer Service and Improvement (to include on Intranet and Internet if applicable to the public)	

1. Introduction

This strategy sets out the ambitions of both Bolsover District Council and North East Derbyshire District Council in the area of information management. Both councils recognise the importance of information to the daily work of the authorities. Organisations gather information for the prime purpose of record keeping or making decisions. We do this by summating, aggregating and analysing data flowing through our operational systems. This is then used to form the basis of evidence based decision making. By processing data and putting it into context we derive information, which we use to run our business. Intangible qualities such as knowledge and wisdom also help to shape information.

Information is gathered from a variety of sources, including customers, clients, stakeholders, government and partners. Information is a key resource, which if properly managed has a crucial role to play in enabling better decision making and delivering effective services to the community.

Types of information held may include financial data, property data, employee data, customer records, consultation data, equality data, polices, procedures, decision documents, transactional data, spatial data, publicity information etc. This information is captured in many different formats including letters, emails, reports, leaflets, web content, data sets, databases etc.

Councils must have in place an effective framework for collecting, accessing, storing, sharing and deleting information. It is even more important to have a consistent approach at times when both Councils are continuing to experience budget pressures. Information technology has a huge role to play in providing and managing information.

This strategy aims to outline our approach over the next three years.

2. Principles

Information is a critical resource which must be effectively managed by the business in order for the councils to meet strategic aims, whilst meeting its obligation to the public. Taking into account our legislative, performance and policy responsibilities, the following key principles have been designed to set the direction of the information management strategy:

- Information is actively and strategically managed as a critical business asset
- Standard policies and procedures will be in place to implement legislative and regulatory requirements
- We understand the information we have available and who is responsible for it
- A strong focus on data quality is important to ensure information is accurate

- Storage and security of information is managed effectively
- Employees have the necessary skills to manage and use the information resources we hold
- Availability and accessibility of information is managed efficiently to promote transparency
- Sensitive or restricted or personal information is managed safely and information sharing is carried out with confidence
- We will continuously strive to improve our information management systems.

These principles will apply to all aspects of the councils work.

There are a number of national drivers which influence this strategy and the above principles. These include:

- Legislation and regulatory requirements (see below)
- Public Service Network (PSN) requirements
- Payment Cards Industry(PCI-DSS) requirements
- Contractual requirements such as the Public Sector Mapping Agreement and Data Co-Operation Agreement.

The main legislation that guides this strategy is:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Regulation of Investigatory Powers Act 2000
- Re-use of Public Sector Information Regulations 2005
- Public Records Act 1958
- Local Government Act 2000
- Code of Recommended Practice for Local Authorities on Data Transparency (2011)
- E.U. INSPIRE Directive 2007/2/EC.

The ownership and governance of this strategy will be through the following model:

Governance Role	**Responsibility**	**Officer(s)**
Strategic Sponsor	High level sponsorship of the strategy and its implementation	Executive Director (Transformation)
Information Governance Board	Sets the strategic direction for information management and monitors progress	Executive Director (Operations)/ Joint Assistant Director – Customer Service and Improvement/ ICT Manager /other nominated officers
Strategic Information Owner	Co-ordinates the delivery of the information management strategy	Joint Assistant Director – Customer Service and Improvement
Information Custodians	Ensuring the effective collection, storage, access, sharing and deletion of information within departments	Assistant Directors and Service Managers

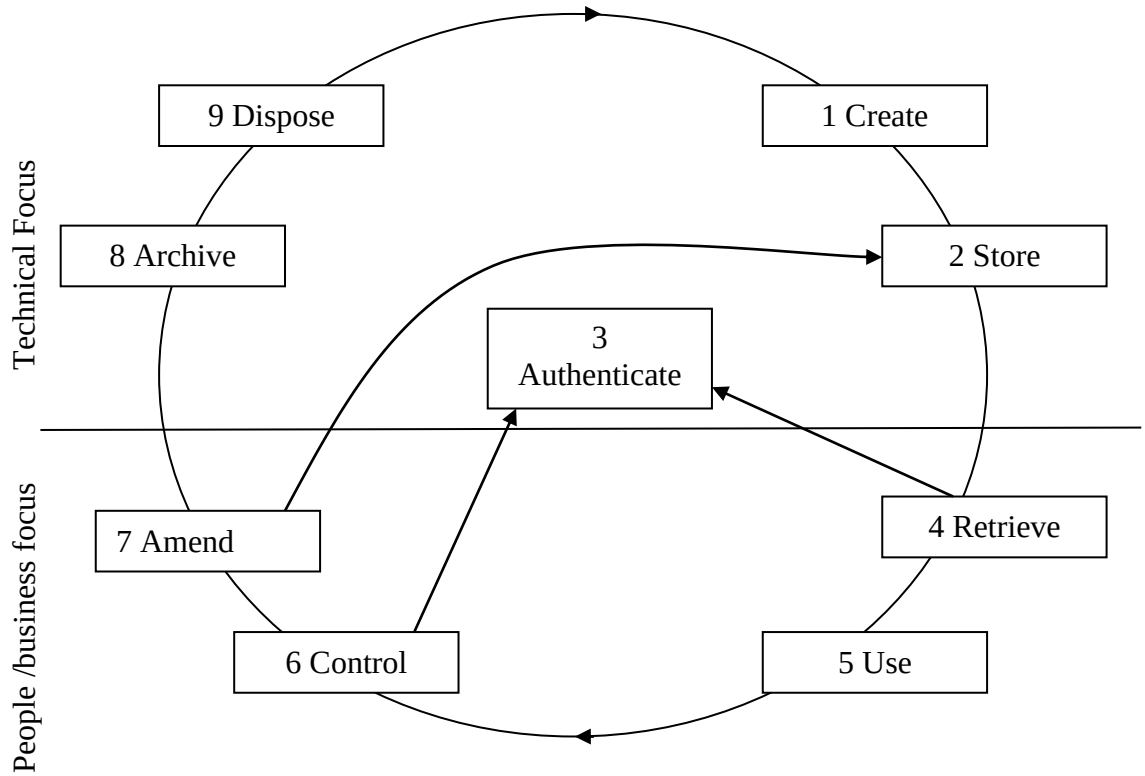
Information Users	Safe and secure day to day authorised access and management of information	All employees and members
Senior Information Risk Owner	Corporate Risk Management	Executive Director (Operations)

3. Information Management Requirements

Managing information involves a controlled and disciplined approach to looking after information assets at every step from creation through to disposal or indefinite retention to archive. High profile information losses from a range of both central and local government authorities and the introduction of financial penalties by the Information Commissioners Office have only served to heighten the need for strong information management in the public sector.

In order to understand our information management requirements we must first identify how we obtain, use and dispose of information within the business. SOCITM have produced a model which sets out the different stages of the information life cycle which are helpful in clarifying information management.

3.1 Information Life Cycle Model (SOCITM 2010)



The information life cycle model consists of:

1. Create	• Both systems and people create information. • Systems do so in an organised way whereas individuals are less so. • Making information available to those who have a legitimate right of access is imperative. • It is also important to avoid overloading people with information.
2. Store	• The important point of storing information is the ability to retrieve it easily later. • Information should be stored securely in line with policy.
3. Authenticate Access	• Security clearance needs to be in place for those that have a legitimate need to access information. • Setting up technical systems and rules about authentication is important. • Secure marking is also becoming an important element.
4. Retrieve	• Retrieval is easier through electronic systems rather than manual files. • Research and retrieval tools should be utilised wherever possible.
5. Use	• Information will be used on a daily basis by employees and contractors to deliver services to customers. • Systems that process and present information need to support the user needs. • Information presented to customers must be easy to understand. • Information transfers within the organisation or with partners must occur in a secure manner in line with Information Sharing Protocols.
6. Control	• Control is about establishing ownership, rights and responsibilities in relation to information. • Personal information (data) as defined by the Data Protection Act has to be strictly controlled. • Data sets should carry protective security markings. • Periodic and random audit checks on data quality and integrity should take place. • Data cleansing should be an ongoing activity.
7. Amend	• Amendments can be by employee interaction or automated. • Clear audit trails should exist when customer records are amended. • Information contained in documents or data sets should have clear version controls.
8. Archive	• Archiving involves the removal of information to avoid clutter and preservation for future access. • The Disposal and Retention Guidelines take effect at

	this point in the life cycle. • Archived documents must be ordered and readily retrievable.
9. Dispose	• At the final stage of the life cycle is the thorough destruction and disposal of information which must be done securely in line with guidelines.

For any model to be successful it needs to be backed-up with policies, procedures and employee learning/development.

3.2 Information Management Policy and Procedures

There are a number of policies and procedures in place which help maintain the security of Council information assets. It is important that all employees are aware of their individual responsibilities to ensure that information relating to them, the Council and its customers, is protected.

The ICT policies are currently under review and will be made available on the intranet shortly.

Freedom of Information (including Data Protection and Environmental Information Regulations) policies and procedures can be found on the intranet.

Employees need to be aware of their own personal responsibilities, be prepared to report behaviour that is not in line with good information management and understand the outcomes for breaching information management controls.

3.3 Employee Learning and Development

Prior to recruitment information management skills should be considered as part of the recruitment and selection process for potential employees. It is also important that competencies identify information management as a core skill set to be discussed in the employee appraisal process.

All employees will be required to attend mandatory Data Protection briefings every three years; these were last delivered in December 2013. New starters will be offered briefings within 6 months of starting employment.

All employees will be required to attend Security Awareness training provided by ICT every three years. The next sessions will be offered during 2014. Thereafter new starters will be covered as part of the IT induction.

4. Strategy Action Plan

In order to ensure that this Information Management Strategy is delivered there are a number of key developments which need to be implemented. These will be defined within this section.

4.1 Public Service Network (PSN) Compliance

The Public Service Network (PSN) is a secure wide area network (WAN) that allows access to Central Government systems, secure data transfer, secure email and accredited solutions provided by public sector organisations and accredited third parties. At present this includes GCSx secure email, CIS (Benefits), Tell Us Once and Electoral Registration systems. The scope of the PSN network covers local authorities, central government departments, National Health Service, the Criminal Justice Extranet and the Police National Network. Some council employees will be required to have access to the facilities operated by this network in order for them to carry out their business. This may include employees having access to secure email facilities. All users requiring access to the PSN network will be required to read and understand an Acceptable Usage Policy (AUP) and sign a Personal Commitment Statement.

In order to be PSN complaint the Council has to ensure that a number of conditions and controls are in place. These are subject to annual review by the PSN team within the Cabinet Office based on submissions stating our compliance with the controls. In addition a 3rd party external audit is undertaken to test a number of the technical security controls within the Code of Connection.

Further information can be found in the Information Security Policy.

In order to address the issues generated by Public Service Network compliance we will:

- Approve this joint Information Management Strategy 2014- 2017 and deliver the agreed implementation plan.
- Establish a joint Information Governance Board by May 2014.
- Perform full Baseline Personal Security Standard (BPSS) checks for all PSN service users from January 2014 and for all users by January 2015.
- Revise the Information Security Policy in June 2017 or before if significant changes occur.
- Deliver annual training to all PSN users.
- Continue to deliver an annual Data Protection Work Programme to ensure changes in legislation and practice are reflected in council procedures.
- Deliver three year refresher training in Data Protection by December 2016.
- Deliver refresher Security Awareness Training for all staff during 2014 and then on a three yearly basis, this may be officer led or on-line.
- Deliver regular Security Awareness Training for all new staff, members or 3rd parties with access to our corporate network.

4.2 Information Asset Management

Information is a major asset that the Council has a responsibility and requirement to protect. Protecting information assets is not simply limited to covering the stocks of information (electronic or paper records) that the councils maintain it also covers the people who use them, the processes they follow and the physical equipment used to access them.

Currently neither authority has a complete list of systems (manual or electronic) processing personal data and therefore no inventory of the information assets it owns.

The new proposed EU Data Protection Regulations identifies the need for complex organisations to hold a record of all processing of personal data. Personal data is any information about any living, identifiable individual. Under the new regulations, Data Protection Officers have to be accountable for all Council systems/data bases containing personal data/information. The new regulations also require the Council to consider data privacy and recommend the introduction of Data Protection Privacy Impact Assessments. Guidance on conducting Privacy Impact Assessments has been produced and templates are in place. The assessment however is quite detailed and requires specialist knowledge of Data Protection legislation.

The storage and archiving of information assets is an important element which can often be overlooked. The important point of storing information is the ability to retrieve it easily later. Effective archiving involves the removal of information to avoid clutter and preservation for the future. All archived documents must be ordered and readily retrievable. Both councils are at different stages in relation to storage of manual records. Work is necessary at North East Derbyshire to improve this aspect of information management, although a review at both authorities would be timely to ensure space is being utilised appropriately.

In addition the storage of electronic data both within business system databases, structured data, and in unstructured data form, e.g. Z: and L: drives and personal data folders needs reviewing with regards to both data retention, duplication of data and data security.

Work has recently been undertaken to improve the deletion and disposal of data within both councils. Guidance has been produced and awareness increased through briefings. These improvements will be kept under review.

Both councils have in place Data Protection Breach Management guidance and processes for reporting data breaches. A breach is considered as the loss, release or corruption of personal (customer or employee) data. After notification of a breach consideration has to be given to if the breach is serious enough to warrant reporting to the Information Commissioners Office. The extent of the harm is judged on the volume of personal data involved and the sensitivity. Having adequate breach management is important to ensuring compliance with the Data Protection Act.

In order to address the issue of Information Asset Management we will:

- Work with departments to assign information asset owners and create a Personal Data Asset Register for each Council by March 2015.
- Work with departments to complete Data Protection Privacy Impact Assessments on more complex systems holding personal data or on the implementation of new ICT systems.
- Carry out regular Internal Audit checks on departmental systems identified in the Personal Data Asset Register.
- Carry out a review of storage and archiving at both Councils and make recommendations to SAMT by December 2014.
- Carry out a review of electronic storage at both Councils and if necessary make recommendations to SAMT by December 2014.
- Continue to promote and monitor the Data Protection Breach Management log to inform decisions about self reporting to the Information Commissioners Office.

4.3 Information Classification

In relation to Central Government ICT systems all information assets must be classified and labelled in accordance with the HMG Security Policy Framework (SPF). The classification determines how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should clearly indicate the classification. At present the councils have not implemented corporate document classification. However users may come in contact with documents classified under the government scheme. Some Council departments who work with government departments will be familiar with the classifications and will be using them on a regular basis.

The Government Security Classifications are commonly known as a 'marking scheme'. A new marking scheme comes into effect from April 2014. These are:

- OFFICIAL
- SECRET
- TOP SECRET

The classification pre April 2014 may remain in circulation and are:

- Unclassified
- PROTECT
- RESTRICTED
- CONFIDENTIAL
- SECRET
- TOP SECRET

PROTECT, RESTRICTED (old) or OFFICIAL (new) are the markings which are applicable to local government.

A limited subset of OFFICIAL information could have more damaging consequences (for individuals or the organisation generally) if it was lost or stolen or published in the media. Where there is a clear and justifiable requirement to reinforce that the access to the information is on a need to know basis the information asset should be marked OFFICIAL-SENSITIVE.

In certain circumstances the OFFICIAL-COMMERCIAL marking can be used for example market-sensitive information which could be damaging if improperly accessed, including that subject to statutory or regulatory obligations. OFFICAIL- PERSONAL can also be used for particularly sensitive information relating to an identifiable individual, where inappropriate access would have damaging consequences e.g. Vulnerable individuals.

PROTECT, RESTRICTED or OFFICIAL information must not be disclosed to any other person or organisation via any method including, but not limited, to the following:

- Paper based methods
- Fax
- Telephone.

Where it is disclosed/ shared it should only be done so in accordance with a documented Information Sharing Protocol and /or Data Exchange Agreement. Disclosing PROTECT, RESTRICTED or OFFICIAL information (subject to descriptor) to any external organisation is also prohibited, unless via the Government Connect Secure Extranet (GCSx) email. Where GCSx email is available to connect the sender and receiver of email messages this must be used for communicating PROTECT, RESTRICTED or OFFICIAL information (subject to descriptor).

Guidance on the use of classifying information can be found in the joint Information Security Policy and on the intranet.

In order to address the issue of Information Classification we will:

- Communicate to all PSN Service users the new Government Security Classification scheme prior to April 1st 2014 when they are adopted by Central Government.
- Review the new Security Classifications for potential adoption within the Strategic Alliance. This may require clarification of descriptors against the OFFICIAL classification which is the only classification that would apply.
- Identify and record data classified as PROTECT, RESTRICTED (old standards) or OFFICIAL (new standards) within the Personal Data Asset Register.

4.4 Data Transparency

The Government is keen for local authorities to routinely publish information and datasets which are of interest to the public and/or have been requested under a Freedom of Information request.

The Government's Transparency Programme and Open Data agenda requires us to publish datasets that have been requested under the Freedom of Information Act 2000 and to publish information in accordance with the Code of Recommended Practice for Local Authorities on Data Transparency. Government is considering making this Code mandatory during 2014.

Bolsover has a dedicated webpage for data transparency which contains the information listed within the Code together with other datasets we have identified through Freedom of Information requests. Information on this page is available to use under the Government's Open Government Licence. The trend towards publishing more information will increase and both Councils need to be aware of this ongoing requirement.

In order to address the issues of Data Transparency we will:

- Continue to develop the availability of datasets at Bolsover District Council in line with the transparency programme.
- Develop a dedicated webpage for data transparency at North East Derbyshire District Council by December 2014.

4.5 Local Land and Property Gazetteer (LLPG)

The authorities are required to hold and maintain a database on all land and property within the districts as part of the DCA (Data Cooperation Agreement). The DCA is issued by GeoPlace™ LLP (a partnership jointly owned by the Local Government Association (LGA) and Ordnance Survey. This database, known as the LLPG (Local Land and Property Gazetteer) must be maintained to a specified standard in order to form part of a central, national database/gazetteer and the authority must have a designated Authority Address Custodian who is responsible for ensuring the LLPG is managed correctly. The LLPG at both BDC and NEDDC is also the corporate address database which should be linked to all address based systems in order to streamline processes and improve efficiency with regards to address management across the authorities.

In order to address issues around LLPG we will:

- Maintain the LLPG to the required standard.

4.6 Geographical Information System (GIS)

Spatial data is essential for a local authority to perform many of its statutory functions, in its simplest form this is geographical or map data. In order to use internally created spatial data and Ordnance Surveys base mapping, the authorities are signed up to the PSMA (Public Sector Mapping Agreement) which governs which data we can use, how it can be used and allows us to share Geographical Information (G.I.) or mapping with third parties in order to meet our core business requirements. The PSMA requires authorities to designate and Authority Principal Contact who is responsible for ensuring that data is managed and maintained/managed correctly and copyright is protected.

A PSMA Contractors licence is required (essential) for any situation where G.I or LLPG data is required by third parties, consultants and contractors. The designated Authority Principal Contact is responsible for issuing the data and licences.

It is essential for user and departments/service areas that create and maintain G.I. data, to have a strong level of data management knowledge and awareness.

In order to address issues around the GIS we will:

- Ensure that the requirement of the Public Sector Mapping Agreement is met.

4.7 INSPIRE Directive

European Directive 2007/2/EC is known as 'INSPIRE', establishes an infrastructure for spatial information in the European Union. Under INSPIRE authorities must make available in a consistent format, spatial datasets and metadata which come within the scope of the Directive and also create network services for accessing the datasets. These datasets must be created to a specified E.U. wide standard in order for the data to be shared throughout Europe.

No personal data would be shared under this requirement.

In order to address issues around the INSPIRE Directive we will:

- Ensure that the requirements of the INSPIRE Directive is met.

5. Glossary of terms

- **Baseline Personal Security Standard** (BPSS) check is a set of minimum requirements for checks and validation of employees. The full checks, including unspent convictions, need to be undertaken for PSN service users in 2014 with an extension to all ICT users from January 2015.

- **Content** is the umbrella term used to refer to any information asset.

- **Custodians** are the employees delegated by the owning organisation to look after, and take responsibility for, managing and safeguarding an information asset, and this person (or role) will be included in the metadata tagged to the asset. Custodians can authorise amendment and disposal of information assets.

- **Data** are pure facts – devoid of context they have no meaning.

- **Data Protection Privacy Impact Assessments** are a way of accessing systems and processes to ensure that data protection is fully considered and privacy of individuals is not breached.

- **Data Subject** is the individual to whom personal data refers.

- **Information** is data in context, or data processed in order to give it meaning.

- **Information Governance Board** is composed of senior managers representing all functions of the organisation, and takes overall responsibility for information management policy, investment, training and practice.

- **Information owners** in organisations are the corporate body of all information assets. The organisation (through the information governance function and the SIRO) will formally delegate the responsibilities for this role to a named individual (the custodian) with sufficient seniority and authority.

- **Knowledge** is non-codified information stored in someone's brain. It is personal to the owner, being assembled through the filters that person has acquired through their life experience.

- **OFFICIAL information** is the majority of information created or processed by the public sector. This includes routine business operations and service, some of which could have damaging consequences if lost, stolen or published in the media. There is no requirement to mark routine OFFICIAL information.

- The **Public Services Network** is a secure wide area network (WAN) that allows access to Central Government systems, secure data transfer, secure email and accredited solutions provided by public sector organisations and accredited third parties.

- **SECRET information** is very sensitive and justifies heightened protective measures to defend against threat factors. It is usually associated with central government departments such as the military.

- The **Senior Information Risk Owner** is a named individual responsible. In the Local authority context this would usually be the Section 151 Officer or member of Senior Management responsible for risk management

- **TOP SECRET information** is the HM Government most sensitive information requiring the highest level of protection from the most serious threats. It is usually associated with central government departments dealing with national security.

- **User is** any individual with the right and the business need to access an information asset or record.

- **Wisdom** develops from the repeated application of knowledge to problems and issues resulting in outcomes that are widely acknowledged to have been successful by relevant stakeholders.

6. Appendices (if applicable)

- (Joint) Information Management Strategy Action Plan

(Joint) Information Management Strategy Action Plan

Action	Owner	Lead Officer(s)	Target Date	Expected Outcome	Resources
Establish a joint Information Governance Board by May 2014	Executive Director of Operations	JAD- CS&I	May 2014	Established governance Six monthly meetings PSN Service compliance	Officer time
Perform full Baseline Personal Security Standard (BPSS) checks for all PSN service users from January 2014 and for all users by January 2015	JAD – HR & Payroll	JAD – Finance, Revenues & Benefits for funding HR Advisor for checks	January 2015	PSN Service compliance. Ability to continue to deliver key front line services(Benefits/ Elections)	(Compulsory) Cost £3,750 now and further £20,000 for compliance by January 2015
Revise the Information Security Policy in June 2017 or before if significant changes occur.	Executive Director of Transformation	ICT Manager	June 2017	Policies which are up-to-date and fit for purpose	Officer time
Deliver three year refresher training in Data Protection by December 2016	JAD- CS&I	CS&I Team	December 2016	Delivery of mandatory refresher training to ensure compliance with Data Protection Act. Competent employees	Officer and employee time
Deliver refresher Security Awareness Training for all staff	ICT Manager	ICT Manager	December 2014	Ensure compliance with PSN controls	Officer and employee time. Training costs to be identified.

Action	Owner	Lead Officer(s)	Target Date	Expected Outcome	Resources
Work with departments to assign information asset owners and create a Personal Data Asset Register for each Council by March 2015	JAD- CS&I	CS&I Team	March 2015	Compliance with new EU Data Protection Regulations (due 2014)	Officer time. Departmental officer time
Carry out a review of storage and archiving at both Councils and make recommendations to SAMT by December 2014	JAD- CS&I	CS&I Team	December 2014	Report with recommendations. Improved data storage	Officer time. Could incur cost for improved storage solution
Carry out a review of electronic storage at both Councils and if necessary make recommendations to SAMT by December 2014	ICT Manager	ICT Manager	December 2014	Report with recommendations. Improved electronic data storage	Officer time
Communicate to all PSN Service users the new Government Security Classification scheme prior to April 1st 2014 when they are adopted by Central Government	ICT Manager	ICT Manager	March 2014 (complete)	PSN Service compliance	Officer time
Develop a dedicated webpage for data transparency at North East Derbyshire District Council by December 2014	JAD- CS&I	CS&I Team	December 2014	Compliance with Government Transparency agenda. Open data	Officer time