APPENDIX A

Information Governance (IG) Strategy

2012/13 – 2015/16

1. Introduction

1.1 This strategy describes the development and implementation of a robust Information Governance (IG) framework needed for the effective management and protection of organisational and personal information.

1.2 Information Governance describes the approach within which accountability, standards, policies and procedures are developed, implemented and maintained to ensure that all types of information used by the council are held, processed, communicated securely and legally.

1.3 Information is a vital asset for the Council, supporting both day to day operations and the effective management of services and resources. Therefore it is essential that all Council information is managed effectively within a robust governance framework.

1.4 In developing this IG strategy the Council recognises and supports:

- The need for an appropriate balance between openness and confidentiality in the management and use of information
- The principles of corporate governance and public accountability and equally places importance on the security arrangements to safeguard personal information
- The need to share customer information with partner organisations and other organisations in a manner consistent with the interests of the customer
- The principle that accurate, timely and relevant information is essential to deliver high quality council services

1.5 This IG strategy forms part of the Council's Information Governance Assurance Framework and is based on the requirements of the HMG Information Assurance Maturity Model and Assessment Framework issued by the Cabinet Office and CESG and the Local Public Services Data Handling Guidelines.

1.6 This strategy will be approved by the Senior Management Team (SMT) and Audit Committee which is a cross party group of councillors. Approval of IG policies that underpin this strategy will be delegated to the SIRO.

2. Strategic Objectives

2.1 The implementation of this strategy will underpin the Councils Co-operative Values.

Co-operative Value	Linked Information Governance Activity
Openness & Honesty	To proactively publish more Council information and make more datasets available To continually improve responses to information requested under information rights legislation
Ownership	Establish more clearly defined information asset owners in service areas To improve the current publication scheme and ensure it meets ICO requirements
Fairness & Respect	Continue to treat all members of the public requesting information in a consistent and respectful manner Ensure 'every contact counts' by improving responses to information requests to ensure they are easy to understand and answer queries raised
Involvement	Ensure that the community receives information, both proactively and where requested, that enables them to participate in discussion and challenge the council where they feel necessary Make all parties who give/collect information aware of what will happen with the information and give choices in respect to this where possible.

2.2 Government guidance states that the following areas, as a minimum, should be included in an information governance strategy:

- Leadership and governance
- Training, education and awareness
- Information risk management
- Life cycle of information assurance
- Assured information sharing
- Compliance

3. Leadership and Governance

Strategic Aim –
'SMT proactively engages in leading, championing and monitoring information assurance across the council to ensure cultural behaviours in embedding the information governance assurance framework'.

3.1 Without effective senior level leadership and adequate governance arrangements in place, service areas may experience difficulty in factoring information assurance activities in both their medium/long term planning.

3.2 To achieve this strategic aim the following objectives must be met:

REF	Objective
1	Formally establish and embed a number of key information assurance \ governance roles and responsibilities including: • Senior Management Team • Senior Information Risk Owner (SIRO) • Caldicott Guardian • ICT Security Group • Information Asset Owners (IAO's) • Audit Committee See Appendix 1 for expected responsibilities for each of these roles
2	SMT to be aware of all key information assurance risks affecting key corporate systems
3	SMT and the Audit Committee will receive regular reports of progress against information governance strategic aims and objectives
4	IG strategy is aligned with other major council strategies
5	A benefits appraisal of the IG work programme is undertaken to evaluate investment in IG areas

4. Training, Education and Awareness

Strategic Aim –
'Accurate details of training received by all staff are collated and reported to the IG Team Leader on behalf of the SIRO. Surveys show that staff attitudes and behaviours towards IG are aligned to the needs of the council'.

4.1 It is important for all council officers, particularly those with key responsibilities as detailed in 3.2 above, to be empowered to fulfil the requirements of this strategy and associated information governance policies.

4.2 To achieve this strategic aim the following objectives must be met:

REF	Objective
1	An IG training plan is in place that meets the needs of the council and in particular services that process significant volumes of personal and sensitive information.
2	Accurate records are maintained of staff that have completed IG training. Records are collated and reported to the SIRO
3	An assessment is made of the coverage and effectiveness of IG training and awareness programme
4	Specialist training programmes (including information risk management) are in place for staff holding key IG appointments, i.e. those detailed in 3.2 above

5. Information Risk Management

Strategic Aim –
'Information risk is managed throughout the council in a structured way so that senior management understand the business impact of IG related risks and manage them effectively in consultation with relevant third party organisations'.

5.1 All officers are responsible for managing information risk.

5.2 The SIRO has a corporate responsibility for providing a focal point for information risk management. The SIRO does not fulfil this responsibility personally but delegates responsibility to the IG Team, IAO's and ICT Security Group.

5.3 To achieve this strategic aim the following objectives must be met:

REF	Objective
1	The SIRO/SMT are aware of key information assurance risks affecting all systems
2	The SIRO ensures proportionate measures are in place to mitigate information assurance risks
3	External organisations who share information with the Council are satisfied with the level of risk exposure relevant to services they share with
4	Key risk vulnerabilities common to more than one system are assessed and communicated corporately
5	Privacy impact assessments (PIA) are undertaken for all new information systems that process personal information. A risk based programme should also be devised to ensure that retrospective PIA's are undertaken on already established major systems that process personal information.
6	The SIRO/SMT determine the risk appetite for information assurance through delegated authority to IAO's
7	Processes are in place to conduct operational and technical risk assessments of information systems and associated policies/processes

It states that PIA's should be undertaken for new information systems and doesn't state that they should be done for existing systems. However, the major systems, where we hold our most sensitive data (Children's/Adult's etc) are unlikely to be replaced for a long time. If PIA's are designed to ensure the security of our data, should there be a programme to undertake PIA's for all systems to ensure the security of most sensitive data

6 Life Cycle of Information Assurance

Strategic Aim -
'A full range of information governance measures should be implemented that are cost effective and reduce the vulnerability to information security issues throughout the life of the use of information and its eventual destruction'.

6.1 All relevant employees that handle information are expected to understand information flow and employ through life information governance controls which covers information collection, retention, disposal and/or communication of information to third parties.

6.2 To achieve this strategic aim the following objectives must be met:

REF	Objective
1	Details exist of the status of information governance control measures which impact on all key information system and information assets which are made available to the SIRO and SMT
2	Profiles of service areas/information systems exist which map information assurance incidents and key vulnerabilities
3	ICT information is used to predict future service demand and therefore effectively map adequate information governance measures
4	Appropriate back up, business continuity and disaster recovery arrangements are in place and have been tested for all information systems
5	A digital continuity risk plan is in place that encompasses an annual review of all information assets
6	Contracts in place with third party suppliers should detail conditions in respect to digital continuity
7	A scaleable and future proofed authentication methodology is in place for all information systems
8	A plan is in place for the prevention, detection, and resolution of information assurance vulnerabilities including suitable penetration testing
9	A patching policy is in place that includes third party suppliers and details the distinction between routine, critical and emergency patching. It also includes the requirements for information on malware incidents to be collated and reported

10	A corporate information retention schedule is embedded and complied with by all council services

7 Assured Information Sharing

Strategic Aim -
'Information is appropriately shared within the Council and with external bodies / individuals in an assured and cost effective way that maximises the benefits delivered by sharing information, whilst reducing the business impact should a compromise occur'.

7.1 Information sharing is essential part of Council business. It allows more efficient, joined up services to be delivered to the community by the Council and/or strategic partners to benefit customers receiving these services. However sharing information can lead to vulnerabilities particularly if it not being undertaken in a controlled and managed way

7.2 To achieve this strategic aim the following objectives must be met:

REF	Objective
1	Mechanisms are in place to protect information in transit
2	A protective marking scheme exists for all information assets
3	Profiles of service areas/information systems exist which map information governance incidents and key vulnerabilities
4	Agreed policies are in place in respect to information sharing
5	Information sharing agreements should be in place with third party organisations where regular sharing occurs

8 Compliance

Strategic Aim:
'Effective compliance mechanisms provide positive assurance that Council policies are being implemented in an effective way to achieve the desired outcomes'.

8.1 Without effective audit and compliance mechanisms those IG control measures which may cause inconvenience are likely to be ignored resulting in an increase in the risk to the Council's information.

8.2 To achieve this strategic aim the following objectives must be met:

REF	Objective
1	The SIRO is satisfied that the Council is complying with relevant IG legislation

2	A compliance programme is in place that has been agreed by the SIRO and is regularly reviewed
3	Weaknesses identified from compliance reviews are rectified with lessons learnt being reported to the SIRO, SMT, across the Council and to the Audit Committee.
4	A process is in place that brings together all IG related control processes so that a single view can be reported to the SIRO/SMT

Appendix 1

Formally establish and embed a number of key roles and responsibilities including:

- **Senior Management Team/Members** – provides the correct 'tone at the top' for the council in relation to information governance
- **Senior Information Risk Owner (SIRO)** – A member of SMT who is accountable for
    - Fostering a culture for protecting and using data
    - Providing a focal point for managing information risks and incidents
    - Is concerned with the management of all information assets.
- **Caldicott Guardian** – Are appointed to develop and maintain responsible, appropriate and secure practices for sharing and handling of personal health and social care information. .
- **Audit Committee** – The Audit Committee considers the effectiveness of the Council's governance processes and their compliance with legislation and best practice including the information security framework
- **Information Governance (IG)** – The IG team provides a number of key functions including:
    - Advice and support to the council in respect to all information governance matters
    - Co-ordinating all information requests received under information rights legislation
    - Checking for corporate compliance with agreed information governance policies and procedures
- **ICT Security Group** – Group includes a number of key officers in the council and is chaired by the Audit & Information Governance Service Delivery Manager. The groups remit is to discuss and monitor information security/governance issues and compliance across the council and report significant issues to SMT.
- **Information Asset Owners (IAO's)** – All service areas have information assets, some have more than others. IAO's are part of the senior management in service areas, e.g. for leisure information the IAO's would be the Leisure Facilities & Services Service Delivery Manager and Assistant Director: Environmental & Leisure Services. The IAO is responsible for ensuring information assets in his/her area are adequately protected/risk assessed, managed under statutory obligations and that their value to the council is fully exploited