APPENDIX 2(B)

Information Asset Owner's (IAO) Quarterly Information Risk Return

IAOs (Heads of Service) must complete the following risk return by **20 June 2013** and submit it along with the updated Service Area Risk Register to the Senior Information Risk Owner (SIRO) in order for the Council's Annual Information Risk Return to be submitted to Members.

IAO name		**Signature**	
Service Area		**Date**	
Directorate			
I have reviewed the information risk register for my service area.		Yes/No	
I can confirm that the risks are:		The same as the last period/have changed since the last period. If changed, please modify Risk Register, and submit to SIRO.	
I can confirm that the impact/level of the risks are:		The same as the last period/have changed since the last period	
If the impact/level of the risks have changed, please describe.			
I can confirm that the active controls are:		The same/have changed	
If the active controls have changed, please describe.			
I can confirm that the proposed controls:		Have/have not been implemented	
If the proposed controls have been implemented, the impact/level of risk has changed to:			
If the proposed controls have not been implemented, please describe why not, and outline plans for actioning the			

proposed control.	
I can confirm that any new work programmes have been assessed for information risk and reflected in this return.	Yes/No

Reviewing the information Risk Register

1.1 IAOs must review information risks on a quarterly basis and, where appropriate, escalate any risks to the SIRO. At each review consider if existing risks are still relevant, achieve the same score and if new risks have emerged. Even where risks remain the same, it is likely that controls and contingency plans will require updating

1.2 Where an operationally significant risk has been identified the IAO will need to describe the mitigating actions that will be put in place and then assess the residual risk rating, taking into account the additional measures that are being proposed. When the review of the Risk Register is carried out the IAO must take into account when the mitigating actions have been carried out so they can be entered onto the register as control measures.

1.3 As well as existing risks that have already been identified, the review must also consider forthcoming potential changes in services, technology and threats that may give rise to new risks.

Appendix 1 – Information Risk Register

Information Risk Register			Information Asset Owner (Head of Service): ……										
Directorate/Service Area: ……													
Risk ID		**Risk Description**	**Active Controls:**	**Last Period**		**Current**			**Proposed Controls (incl. Date):**		**Target**			**Risk Owner *Control Owner***
				I	**L**	**I**	**L**				**I**	**L**	**Date**	
1	*Risk (Event)*	**Inappropriate disclosure of personal data**	Compliance with Corporate Risk Management Policy and Risk Appetite Statement					*Additional Actio*	Complete data mapping exercise to provide a register of information					

	Cause(s)	Lack of identification of those information assets containing personal data and sensitive personal data. Lack of awareness training. Absence of Information Sharing Protocols (ISPs) or other agreement (e.g. memo of agreement). Failure to double-check contents proposed for disclosure (including data sitting behind Excel or Word docs). Advice on disclosure of information is not sought from line manager and/or Corporate Information Governance Unit.	Obtaining guidance and support regarding incident management from Corporate Information Governance Unit Ongoing data mapping exercise supported by Directorate Information Governance Stewards WASPI ISPs or other arrangements (*Identify arrangement here)* Annual Protecting Information elearning - *(enter current completion rate)* Identified information assurance roles in place *(IAO, Directorate Stewards, Service Area Liaison Officers)*						assets and their attributes. 100% Annual Protecting Information elearning completed by all staff by…... IAO Reference Guide read by IAO and recorded in annual compliance statement by…… Information Assurance Audit compliance by……..				
	Effect(s)	Serious and unwarranted damage and distress to individuals Breach of DPA and infringement of privacy Regulatory, court action or financial penalties Damage to reputation and integrity Cost and resources required to investigate												
2	*Risk (Event)*	**Theft, loss or unauthorised access to information (electronic and systems related**	Compliance with IT Security, Data Protection and FOI Policies Only encrypted laptops,					*al*	Awareness of Data Breach Reporting Procedure raised by emailing all Heads of Service/IAOs					

	Cause(s)	Inadequate access and permissions management Password sharing Poor information asset management Dishonesty Emails sent to wrong address or lost/ compromised during transmission Inadequate business continuity planning	smartphones and USB memory sticks will be used Annual 'Protecting Information' elearning (enter current completion rate) Regular data backups are carried out and up to date backup logs are kept Data Breach Reporting Procedure available and awareness raised amongst staff by Information Governance Stewards.						by……. Implementation of Protective Marking Scheme…….. Review of permissions by…….					
	Effect(s)	Serious and unwarranted damage and distress to individuals Breach of DPA and infringement of privacy Regulatory, court action or financial penalties damage to reputation and integrity Cost and resources required to investigate Cost of recreating / retrieving information												
3	*Risk (Event)*	**Theft, loss or unauthorised access to information (paper based)**	Compliance with IT Security, Data Protection and FOI policies. Annual 'Protecting Information' elearning (enter current completion rate)					*Additional Action*	Data Loss Reporting guidelines issues to all staff by……. Implementation of Protective Marking Scheme					

	Cause(s)	Documents stored in damp conditions and damaged beyond repair Documents not filed correctly and not available to be retrieved Dishonesty / sabotage Carelessness Clear desk policy not enforced Documents posted / faxed to wrong address or lost / compromised during transmission												
	Effect(s)	Serious and unwarranted damage and distress to individuals Breach of DPA and infringement of privacy Regulatory, court action or financial penalties damage to reputation and integrity Cost and resources required to investigate Cost of recreating / retrieving information												

4	*Risk (Event)*	**Ineffective or Insecure Information Sharing internally and externally**	Compliance with Corporate Risk Management Policy and Risk Appetite Statement Obtaining guidance and support regarding incident management from Corporate Information Governance Unit WASPI ISPs or other arrangements (*Identify arrangement here)* Annual Protecting Information elearning - *(enter current completion rate)* Ongoing data mapping exercise supported by Directorate Information Governance Stewards Privacy Impact Assessments completed as appropriate.					*Additional Action*	Complete data mapping exercise to provide a register of information assets and their attributes.				
	Cause(s)	ISPs/agreements not in place or not comprehensive enough Failure to share the right information with the right people at the right time Lack of awareness of what information is held and therefore when/where it could be beneficially shared Shared information is not stored securely (paper or electronic)											

	Effect(s)	Information used for purposes other than those agreed Serious & unwarranted damage and distress to individuals Breach of DPA and infringement of privacy Damage to reputation and integrity Information not shared prior to the departure of staff - knowledge not retained Loss of business continuity	completed as appropriate.											
5	*Risk (Event)*	**Records retained for the wrong length of time**	Compliance with Corporate Retention and Disposal Procedures Ongoing data mapping exercise supported by Directorate Information Governance Stewards					*Additional Action*	Complete data mapping exercise to provide a register of information assets and their attributes. IAO raise awareness of importance of keeping records, one of the organisation's most important resources, correctly. Staff training on effective record keeping					
	Cause(s)	Information not covered by retention policy Lack of awareness Lack of motivation to file records appropriately and regularly Dishonesty / sabotage Records retained 'just in case' Lack of awareness of what information is held and therefore when it should be disposed of.												

	Effect(s)	Breach of DPA, FOI & Public Records Act Breach of other requirements for the retention of records Unnecessary cost of storage of physical and electronic information Inability to protect Council's best interests in cases of litigation because relevant records have been destroyed or can't be found Premature destruction seen as an attempt to prevent disclosure Regulatory, court or financial penalties Damage to reputation and integrity												
6	*Risk (Event)*	**Failure to create or locate reliable records as evidence of business decisions and activities**	Compliance with Corporate Risk Management Policy and Risk Appetite Statement. Compliance with Corporate Retention and Disposal Procedures, and effective review and destruction process Ongoing data mapping exercise supported by Directorate Information Governance Stewards, helps to identify gaps in record keeping that impairs					*Additional Action*	Complete data mapping exercise to provide a register of information assets and their attributes.					
	Cause(s)	Records not created in the first place to document key decisions and activities Records retained unnecessarily result in large volumes of data to be searched if information is requested Records are not managed systematically and electronic and physical filing is not carried out												

	Effect(s)	Breach of DPA and FOI Records required for evidential purposes (i.e. in court) will not be available Inability to defend the Council in any legal action Critical information can't be found or takes too long to find when needed	evidence of Council activity.											
7	*Risk (Event)*	**Information assets, including vital records, lost as a result of fire, flood, server failure, a power loss, etc**	Ongoing data mapping exercise supported by Directorate Information Governance Stewards, helps to identify vital records.					*Additional Action*	Identify vital records and include them within local continuity plans. Complete data mapping exercise to provide a register of information assets and their attributes. Desk top contingency exercise carried out every 12 months				
	Cause(s)	Vital records not identified in local business continuity plan Business continuity plans are not in place												
	Effect(s)	Vital records may be destroyed Unable to access information with potential legal & financial consequences Significant investment required in the case of a major incident or failure Business continuity affected												