Annex A

Corporate Information Governance
Level 1 Information Maturity Model Action Plan

Ref	High Level Action	Ref	Action and Current Position	RAG
1	Promulgate top level policy statement • Publish Information Charter	a	Information Charter is published on the internet. Charter has been reviewed and is up to date	✓
		b	Comprehensive list of Information Governance policies in place	
2	Senior commitment to Information Assurance • Appoint Senior Information Risk Owner (SIRO) • Report to Main Board regularly • Provide assurance to Audit Committee on annual basis	a	SIRO appointed and sits on Main Board.	✓
		b	Annual progress report to CMT – in place	
		c	Annual assurance report to Audit and Governance Committee – in place and on regular agenda	
		d	Develop assurance mechanism to support SIRO assurance report – to be integrated with Annual Assurance Statement	
3	Appoint Information Asset Owners (IAOs) for each key group of information assets	a	Information Asset Groups identified and communications established. 50 key IAOs used as basis for communication	I/P
		b	Continue ongoing awareness training of the key "50" information asset owners	
		c	Continue review of information asset registers and ensure "fit for purpose"	
4	Develop reporting mechanism to provide assurance to SIRO • Breach reporting and investigating system	a	Review and update Data Breach reporting mechanism	I/P
		b	Develop assurance mechanism for IAOs to feed into Departmental	

Ref	High Level Action	Ref	Action and Current Position	RAG
	• IAO assurance to SIRO • Compliance review		Information Governance Champions and annual assurance as part of the Assurance Statement	
		c	Carry out reviews of adherence to Data Breach policy as part of audit programme	
		d	Continue to carry out QA reviews of FoI cases and report to CIGG quarterly	
		e	Develop and implement file management standards to ensure compliance with Legal Admissibility Code of Practice	
		f	Carry out compliance reviews of adherence to LA Code of Practice. Report annually to CIGG and include in annual assurance to Audit and Governance Committee	
5	Carry out annual risk awareness training for those with access to personal data • Identify groups of staff and their training needs • Develop training packs for different groups • Deliver selected training • Monitor delivery of training	a	Continue Shout campaign – include findings from internal audit visits in campaign	**I/P**
		b	Continue with spot checks of compliance with security at West offices and other council establishments	
		c	Develop and implement Metacompliance (Icomply)	
		d	Identify training needs of different groups of staff	
6	Develop data sharing protocols with 3rd party suppliers & delivery partners • Identify groups, exposure and needs • Develop appropriate awareness information packs • Ensure requirement is	a	Ensure robust data sharing protocols exists with partners based in West Offices	**I/P**
		b	Review CYC arrangements against NHS data sharing standards	
		c	Identify and review all partnerships to ensure protocols are in place	

Ref	High Level Action	Ref	Action and Current Position	RAG
	included in contracts • Deliver training where appropriate			
7	Develop Information Risk Policy • Define information risk appetite • Agree classification scheme for records • Communicate scheme to staff • Monitor compliance	a	Classification scheme in place and communicated to staff via Colin	I/P
		b	Conduct QA reviews of Information Asset registers and application of classification scheme	
		c	Develop and implement records management policy	
		d	Implement Legal Admissibility policy	
		e	Develop assurance mechanism for BS 10008	
8	Develop Information Risk Register • Register monitored regularly • Highest risks fed into corporate risk register • IAOs and IMs identified in Information Risk Registers	a	Maintain and update Information Risk Register	✓
		b	Ensure key DP risks continue to be considered as part of corporate and service risk register for CYC	
9	Information Security • Develop Information Security Policy covering both IT and non IT based data • IT Security Officer appointed • Access to and use of sensitive data monitored	a	Ensure policy for home working and bring your own devices is implemented and complied with	✓
		b	BYOD and Home Working policies approved by CIGG	
		c	Review arrangements for IT security compliance monitoring	
		d	Monitor EDRMS Info Gov security arrangements	
10	Data/Information Transparency	a	Review Compliance with Code of Practice – Self Assessment	I/P