RAG Summary of Phase One GDPR Self Audit Monitor Returns

v0.4 February 2019

Dept / Compliance Action	M&CP				DBE				City Surveyors						Schools			DCCS & Comm Safety									Open Spaces						HR	Remembrancers					Chamberlains (Non IT)											IT Services
GDPR Risks	Billingsgate	Smithfield	New Spitalfields	Port Health & Public Protection	Transportation & Public Realm	District Surveyor	Planning Policy	Planning & Development Mgt.	Operations Group	Corporate Property Group	Investment Property Group	Projects	Business Peromance & Directorate	CPAT	CoL S	CoL G	Freemens	People	Barbican Estates	Housing & Neighbourhoods	Housing Benefits	Barbican and Comm Libraries	Commissioning & Partnerships	Property	Public Health	Community Safety	The Commons	Epping Forest	Directorate	Cemetry and Crematorium	WH Park and City Gardens	H Heath / Highgate Wood / QP / KH	All	Busines Support	Parliamentary Counsel	Parliamentary Briefings Manager	City Events	Private Events	City Proc	Anti Fraud	City Revenues	Corp Treasury	Pensions	Dept facing finance units	Payroll	Corp Accountancy	Chamb Court	Directorate	IT Non Systems and Data Security
Areas where there are risks to GDPR compliance such as insecure data handling are notified to AIN reps and the Compliance Team.																																																
Awareness - Communication & Guidance																																																
Any job-specific training needs are identified and being managed																																																
All staff are aware of the GDPR issues and queries process																																																
ROPA and Records Management																																																
Records Retention Schedule in place																																																
Process for updating Retention Schedule is in place																																																
ROPA in place																																																
Process for updating ROPA is in place																																																
Communicating privacy information																																																
Privacy notices (how the City of London Corporation as a data controller collects and uses personal information) are in place																																																
Lawful basis for processing personal data - consent																																																
Records are kept for where consent has been received from the data subject																																																
Contracts																																																
There are written agreements in place for new contracts with third party service providers and processors, including those who process personal data on behalf of the City of London Corporation as a data controller, that ensure the personal data that they access and process is protected and secure.																																																
Data Subjects Rights																																																
All relevant staff are aware of the process for an individuals' requests to access their personal data (SAR , Right to Access)																																																
Guidance is in place to respond to individuals' other rights Right to rectification Right to Erasure Right to Restriction Right to Data Portability Right to Object Right to Object to Automated Decision Making / Profiling																																																
Guidelines for processing children's data are in place																																																
Data Protection																																																
All staff have read the CoL Data Protection Policy 2018																																																
All staff are aware of the Data Protection Impact Assessment Procedure & Guidance																																															
All relevant staff are aware of the process for identifying and reporting a Data Protection breach																																															
Electronic communications conform to PECR (Privacy and Electronic Communications Regulations) i.e marketing by phone, email, text ; use of cookies or a similar technology on the CoL website; or compiling a telephone directory (or a similar public directory)																																																
Guidance in place for transferring data securely outside of the EU																																																
Guidance in place for transferring data securely between CoL and 3rd parties																																																
All staff have read the CoL Security Policy - People																																																

IT Services - Systems and Data Security	
Secure storage arrangements are in place and documented to protect records and equipment in event of loss, damage, theft or compromise of personal data.	
Documented procedure in place to securely dispose of records and equipment when no longer required.	
Hardware and software assets are documented; management policy in place	
Security of mobile working and the use of mobile computing devices in place.	
New and existing hardware configured to reduce vulnerabilities and provide only the functionality and services required.	
Controls in place to manage the use of removable media in order to prevent unauthorised disclosure, modification, removal or destruction of personal data stored on it.	
User accounts to authorised individuals set up to provide the appropriate permissions and access to information.	
Password security policy and rules' in place to detect any unauthorised access or anomalous use.	
Anti-malware defences in place to protect computers from malware infection.	
Routine backs-up of electronic information in place to help restore information in the event of disaster.	
User and system activity logged and monitored to identify and help prevent data breaches.	
Security patching policy is place to prevent the exploitation of technical vulnerabilities	
Boundary firewalls in place to protect computers from external attack	
Personal data (structured and unstructured) and information under management to identify / rectify potential risks to security (Data Discovery)	

Key

Not yet started	
Partially implemented	
Fully implemented	
Not applicable to this department	