MAYOR OF LONDON

OFFICE FOR POLICING AND CRIME

Appendix 1b

DIRECTORATE OF AUDIT, RISK AND ASSURANCE
Internal Audit Service to the GLA

REVIEW OF INFORMATION MANAGEMENT (ACCESSIBILITY OF PUBLIC DATA)

DISTRIBUTION LIST

Audit Team

Prakash Gohil, Audit Manager
Steven Snaith, RSM Tenon Associate Director
Keith Kemmery: RSM Tenon Senior Consultant

Report Distribution List

David Munn, Head of Information Technology
Tom Middleton, Head of Performance and Governance
Albert Chan, Information Governance Manager
Chris Imthurn, Business Manager
David Gallie, Assistant Director of Finance

CONTENTS

EXECUTIVE SUMMARY

1. Background

1.1 This review of Information Management was carried out as part of the internal audit 2011/12 plan. The objective for the Information Governance Team is to support the GLA's compliance with information rights legislation and records including the publication scheme.

1.2 At the outset of the review, the potential risks identified to achieving the objectives of Information Management (Accessibility to Public Data) were:-

- Failure to comply with the requirements of relevant legislation
- Inadequate data classification
- Improper management of information and records
- A lack of approved policies, procedures and information governance strategies
- Failure to monitor compliance and investigate complaints
- Mishandling of subject access requests and exemptions for information
- Inadequate information governance training and awareness

1.3 Information Rights legislation consists of the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulation 2004, all of which are enforced by the Information Commissioner. The GLA records and monitors all formal requests for information on the WriteOn correspondence system.

1.4 The GLA has a legal obligation to comply with the Information Rights legislation and the culture of transparency encouraged by the Freedom of Information and Environmental Information legislation, ensuring a consciousness that the GLA is accountable to tax payers for the way it performs and spends public money.

1.5 Apart from the 'WriteOn' correspondence system that contains a record of all correspondence that is received and sent by the GLA, the GLA also has a number of management information systems including Notify; a system for tracking homeless households that are placed in temporary accommodation by London Boroughs.

1.6 To comply with the Environmental Act, the Borough Air Quality control scheme provides information in respect of air quality across London Boroughs.

2. Audit Assurance

Substantial Assurance

Key risks to information management are being managed effectively, however some controls need to be improved to ensure business objectives are met.

3. Areas of Effective Control

3.1 Responsibility for overseeing compliance with the Data Protection Act, Freedom of Information Act and the Environmental Information Regulations has been formally designated, reducing the risk of the GLA failing to manage compliance with related information governance requirements and resulting legislative penalties.

3.2 We found the scope of the Data Protection policy and associated IT and technical policies to be adequate, reducing the risk of unauthorised or unlawful processing of personal data.

3.3 The Data Protection policy framework incorporates adequate data subject access procedures, reducing the risk that staff are not aware of the process for responding to a data request and not meeting related obligations.

3.4 The GLA Freedom of Information (FOI) and Environmental Information Regulation (EIR) procedures are well designed, incorporating key related legislative requirements, reducing the risk that GLA staff are unaware of their responsibilities for dealing with FOI and EIR requests.

3.5 The design of the GLAs FOI publication scheme is adequate and structured in accordance with the model publication scheme prepared and approved by the Information Commissioner. In addition, the FOI publication scheme is available to members of the public via a page dedicated to Freedom of Information.

3.6 The format of the publication scheme follows the information groups and classes contained in the model scheme approved by the Information Commissioner.

3.7 The control framework for the maintenance of response timeframe records is adequate in providing monitoring information to support regulatory compliance and reduce the risk of censure by the Information Commissioner.

3.8 The GLA Records Management Policy establishes a mandate to apply information and records management rules and procedures across the GLA.

3.9 The GLA Retention Schedule is designed to help all employees dispose of the records they do not need and hold the records they need to retain. It is in a searchable format and can be used to assign a review period or retention code when depositing new records in the off-site records store.

3.10 Policies and procedures relating to information security, covering such areas as system and application access and use of encrypted removable media, provide a suitable data management framework.

4. Key Risk Issues for Management Action

4.1 The GLA notification to the Information Commissioner is renewed on an annual basis, to ensure that it remains current and reflects all processing taking place. To support this, the GLA Data Protection Officer (DOP) periodically requests from each directorate details of the systems used for processing/recording personal information. However, this was last carried out between October and

December 2009 and no formal process for supporting data audits is in place. A lack of an annual data audit increases that the risk that the notification to the Information Commissioner may not reflect all processing that is taking place within the GLA.

4.2 The protective marking scheme policy that has been documented by the GLA in line with the Government Protective Marking Scheme (GPMS) is in draft and has not been implemented. (The establishment of a protective marking scheme is a mandatory requirement for central government within the Governments Security Policy Framework that was launched in December 2008. The current version 7 was issued October 2011. It is considered best practice for other public sector bodies). The lack of implementation of the Government Protective Marking Scheme increases the risk that sensitive information that should not be disclosed is inadvertently passed on, included as an email attachment or information received from a stakeholder is incorrectly handled due to staff not being aware of the correct processes for handling protectively marked material.

4.3 The EU's new privacy and electronic directive law came into force on 25 May 2011.The law requires businesses and organisations to obtain consent from visitors to their websites in the UK for the use of tracking technologies in order to store and retrieve usage information from users' computers. One of the most common forms of this technology is referred to as the use of cookies. However, the GLA website at this time has not been updated to reflect these requirements. The failure to have documented a web cookies policy increases the risk that the legal requirements may not be implemented by the required date. The Information Commissioner has already provided a one year grace period for implementation. Unless implemented this could lead to censure by the Information Commissioner or possible fine.

5. Review Objectives

5.1 The overall objective of the audit was to review the adequacy of controls designed to mitigate the risks relating to information management. In particular we are looking to provide assurance that:-

- An approved information management policy is published and communicated in a manner that is relevant, accessible and properly implemented.
- Key roles and responsibilities have been defined and responsibilities including supervision and security are allocated to named individuals.
- Adequate and approved documentation procedures are set and maintained to support all information management system requirements including adequate IT facilities.
- Management information requirements are clearly stated and appropriately reported.

6. Scope

6.1 We reviewed the effectiveness of the procedures and controls established by the Authority to mitigate the risks associated with information management. We also reviewed the information management framework including review of the publication scheme, procedures for processing information request and data /information storage but we did not cover records management.

7. Compliance with the Requirements of Relevant Legislation

7.1 Responsibility for overseeing the GLA's compliance with the Data Protection Act has been assigned to the Business Manager IT Unit. The responsibility is documented in the job description for the role. Our review of the Business Manager's job description confirmed that the role includes acting as the Data Protection Officer for the GLA and ensuring the organisation complies with the Data Protection Act 1998. Responsibilities include:

- The requirement to ensure interests of individuals are protected by the way personal information is processed;
- Developing and maintaining data protection policies, procedures, and forms;
- Processes to ensure that all GLA staff are aware of their related responsibilities.

7.2 The following Freedom of Information and Environmental Information Regulation responsibilities have been designated:

- Responsibility for overseeing the GLA's compliance with the Freedom of Information Act and the Environmental Information Regulations has been assigned to the Information Governance Manager and is documented in the job description for the role.

- The Information Governance Officer supports the GLA's compliance with the Freedom of Information Act and other information compliance regimes and the responsibility is documented in the job description for the role.

Our review of the Information Governance Manager and Information Governance Officer's job descriptions confirmed that the role includes:

- Developing and implementing effective processes for compliance with the Freedom of Information Act and other information compliance regimes; and
- Processing requests for information.

7.3 The GLA has not designed procedures for informing the Data Protection Officer of any new or changes to existing systems or methods of processing personal data. A lack of procedures for informing the Data Protection Officer of such changes (electronic or manual) increases the risk that the GLA may not be able to ensure that they are processing data in accordance with their notification to the Information Commissioner and related legislative requirements.

Risk and Recommendation

The GLA is not able to ensure that they are processing data in accordance with their notification to the Information Commissioner or legislative requirements. A process needs to be designed for ensuring the Data Protection Officer (DPO) is informed of any changes to the way that personal data is processed, in accordance with the Information Commissioner and related legislative requirements.

Agreed Action

Amended procedures which have previously been used when updating our notification and forms will be made available on our intranet page which will allow staff to inform the DPO of any changes to the processing of personal data.

7.4 We found notification to the Information Commissioner to be up-to-date, reducing the risk of censure for failing to notify the purposes for which the GLA processes personal data. However, during the comparison of the GLA notification with notifications made by other public authorities, we noted that the GLA has not included in its Crime Prevention and Prosecution of Offenders purpose that it operates CCTV systems in premises for the prevention and detection of crime and that data subjects could be members of the public whose images may be captured on CCTV.

Risk and Recommendation

The GLA may be censured by the Information Commissioner for not notifying that it is using CCTV. The GLA needs to notify the Information Commissioner's Office that CCTV systems are operating in premises for the prevention and detection of crime.

Agreed Action

Since the Information Management audit commenced the notification department at the Information Commissioner's Office has been informed via email that we operate CCTV for the purposes of crime prevention and prosecution of offenders.

7.5 The GLA DPO periodically requests from each directorate details of the systems used for processing/recording personal information. However, this is not on an annual basis and the last review was carried out between October and December 2009. Although the GLAs notification to the Information Commissioner is renewed on an annual basis, to ensure that it remains current and reflects all processing taking place, the renewal should be based upon a data audit.

Risk and Recommendation

A lack of an annual data audit increases that risk that the notification to the Information Commissioner may not reflect all processing that is taking place within the GLA. Annual reviews should be undertaken to ensure that the GLA complies with the requirements of the Data Protection Act.

Agreed Action

The DPO agrees to carry out an annual review of the processing of personal data to ensure that our notification reflects all processing taking place and ensure that the GLA responds effectively to subject access requests.

7.6 The GLA has adopted the Records Management Society's Local Government retention guidelines. The schedule is the 2004 edition and was re-issued in 2008. Amendments and omissions to the Retention Schedule are noted in this current edition, until a new version of the schedule has been produced and approved. However, we noted that the name of the Information Governance Manager quoted in the schedule is incorrect.

Risk and Recommendation

The design of the document retention guidelines is adequate in identifying the retention periods for key data that is held by the GLA. However; as the schedule is dated 2004 it should be reviewed to ensure that it is accurate and reflects the latest data retention requirements as there is a risk that data could be retained for longer than necessary in contravention of the fifth principle of the Data Protection Act.

Agreed Action

Since the Information Management audit commenced, the GLA's records retention schedule has been reviewed and updated. A new version has now been approved by senior management and published on the GLA Intranet for staff use.

7.7 The GLA document Retention Guidelines are communicated to staff via the intranet. The Information and Records Management page provides an overview of the purpose of the retention schedule. The regular communication of document retention periods to staff reduces the risk of data being retained for longer than is required.

8. Data Classification

8.1 The GLA has documented a protective marking scheme policy and procedures that sets out the framework to classify documentation/data within the criteria of Protect, Restricted, Confidential, Secret and Top Secret. The scheme was designed to be introduced to provide a common baseline for safeguarding sensitive information that is shared with the GLA by, or will be shared with, Government departments, the Metropolitan Police and other stakeholders who use the Government Protective Marking Scheme (GPMS) The principle of GPMS is that information is marked according to the harm that would result from its unauthorised disclosure, and that information so marked will then be handled appropriately to prevent such unauthorised disclosure. However, the GLA policy and procedures are in draft and have not been implemented.

The establishment of a protective marking scheme is a mandatory requirement within version 7 of the Governments Security Policy Framework and mandatory requirements issued in October 2011 and is considered a model best practice for other public sector bodies (Note: The Governments Security Policy Framework was originally issued December 2008 and has been continually updated).

Risk and Recommendation

The lack of implementation of the Government Protective Marking Scheme model increases the risk that sensitive information that should not be disclosed is inadvertently passed on, included as an email attachment or information received from a stakeholder is incorrectly handled due to staff not being aware of the correct processes for handling protectively marked material. The GLA

needs to reconsider the introduction of a Protective Marking Scheme.

Agreed

The GLA's Governance Steering Group (comprising the Head of Paid Service, Director of Resources, Director of Secretariat and the Monitoring Officer amongst others) will be asked to reconsider whether it is in the best interests of the GLA to adopt a protective marking scheme such as that drafted in 2009.

9. Management of Information and Records

9.1 The GLA has documented procedures for providing secure disposal of IT assets. It has a disposal contract with PHS Maxitech for secure disposal of assets. The contract was signed in 2008 for a 3 year duration with a 1 year extension option. A formal process is in place whereby:

- Certificates detailing the equipment collected by PHS Maxitech are received by the GLA and confirmed to the asset disposal register.
- The certificate also provides details of the serial numbers and specific identity of equipment.
- Certificates are also received from PHS Maxitech confirming that data has been purged to HMG Infosec standards where equipment contained hard drives.

We confirmed by reviewing a sample of disposals that the process was being carried out in accordance with the documented process and that appropriate records of asset disposals are being maintained.

9.2 The EU's new privacy and electronic directive law came into force on 25 May 2011. The law requires businesses and organisations to obtain consent from visitors to their websites in the UK for the use of tracking technologies in order to store and retrieve usage information from user's computers. One of the most common forms of this technology is referred to as the use of cookies. However, the GLA website at the time of our review has not been updated to reflect these requirements.

(Note: the GLA website does contain information explaining how to disable their cookies, but this is no longer an acceptable option). However, we do acknowledge that the minutes of the GLA Steering Group 20 January 2012 noted that a Web Cookies Policy was to be drafted by March 2012 and finalised by April 2012.

Risk and Recommendation

The failure to have a documented web cookies policy increases the risk that the legal requirements may not be implemented by the required time. This could lead to censure by the Information Commissioner or possible fine. The Information Commissioner has already provided a one year grace period for implementation. The GLA website needs to be updated to comply with the EU privacy and

electronic directive law.

Agreed Action

Work has been underway to ensure that the GLA's website and use of cookies complies with the EU changes to the Privacy and Electronic Communication Regulations by the end of the Information Commissioner's grace period at the end of May 2012. Since the Information Management audit started, the GLA's interim Senior Digital Marketing Manager has conducted an audit to check what type of cookies the GLA's website uses and assessed how intrusive the GLA's use of cookies is. This work is now complete.

9.3 The GLA has documented a Data Processor contract that forms part of the terms and conditions of an agreement for processing of personal data. However, the GLA does not maintain records of specific data sharing protocols that may be in place.

Risk and Recommendation

The lack of records of agreed data sharing arrangements increases the risk that data could be shared that has not been approved for sharing, resulting in adverse publicity for GLA and censure by the Information Commissioner. Data sharing protocols and agreements should be reviewed and made available to all users as necessary.

Agreed Action

The DPO and the information governance team will make available advice and templates for data sharing agreements and will adapt the existing notification review forms to include details of any data sharing agreements.

10. Approved Policies, Procedures and Information Governance Strategies

10.1 The information and records of the GLA are its corporate memory and are necessary for good corporate governance; to be accountable and transparent; to comply with legal requirements; to provide evidence of decisions and actions; and to provide information for future decision-making. Although, the GLA has not documented an Information Governance Policy, it has published a Records Management Policy and Data Retention Schedule. It has also provided staff with guidance notes relating to information management. These in conjunction with its other policies and procedures provide mitigating controls in the absence of an Information Governance Policy.

10.2 The GLA has documented a Data Protection Policy, which states the requirement for permitting the processing of personal data under principle one (i.e. on order to process personal data fairly, a data controller must provide individuals with details the purpose(s) for which their personal data may be used and (except in limited cases) obtain the consent of the individual). The policy contains guidance on the way in which the GLA expects staff to comply with the principles of the Data

Protection Act. In order to support the seventh principle of the Act the GLA has documented the following Technology Group Security policies:

- Policy on the disposal of equipment – provides assurance that any data that is on computer hard drives is removed reducing the risk of unauthorised access to personal or confidential data;
- Network Services Agreement;
- Processes for authorising information processing - access to systems policy – includes processes for ensuring that all system/application access is appropriately authorised;
- Policy on the use of mobile assets – includes instructions for configuring IronKey encrypted USB drives that reduces the risk of confidential data falling into the wrong hands;
- Business interconnection policy;
- Cryptographic control policy;
- Guidance on the use of Authentication;
- Procedure for incident Management;
- Reporting security concerns; and
- Collection and preservation of evidence.

We found the policies and procedures in place are adequately designed and reduce the risk that staff will not be aware of the GLA's requirements for handling and managing personal data in a secure manner.

10.3 The GLA has not designed a Freedom of Information Act (FOI) policy. However, the following compensating controls are in place:

- The GLA intranet provides a definition of the FOI and the Environmental Information Regulations (EIR), and the responsibilities of staff for complying with requirements of the Act.
- The intranet page also provides links to further FOI documentation e.g. Guidance for GLA staff, Standard response templates, Guidance for London Assembly Members and FOI performance monitoring.
- The Information Governance guidance for the Mayor and London Assembly Members provides guidance in identifying information that will constitute information held by the GLA, what will constitute personal information and what will constitute information belonging to a political party and the implications for each under the information access legislation.

- The GLA website also provides for the general public details of the GLA obligations under the FOI and EIR and the method to be employed to obtain information. Details of the potential charges are also stated.

10.4 The GLA has adopted the model publication scheme approved by the Information Commissioner and available on the ICO website. It is available to the general public via the GLA website under a Freedom of Information heading. The publication scheme commits a public organisation to proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the organisation and falls within the classifications stated in the scheme. We confirmed that:

- The GLA does routinely publish via its website information in line with the statements contained in the scheme,
- The format of the publication scheme followed the information groups and classes contained in the model scheme approved by the Information Commissioner.

10.5 The GLA has not carried out an information audit to support the publication scheme. However, to address this issue the GLA has established a Records Management Policy and GLA Records Retention Schedule, together with Information Management policies and staff guides covering particular topics (Managing shared folders, keeping records for corporate requirements, managing emails, intranet social media guidelines) have been documented in order to formalise a framework. In addition, information is covered as a mandatory aspect of all staff induction sessions.

11 Monitoring Compliance and Investigate Complaints

11.1 Independent records of FOI requests and Data Protection subject access requests are maintained using spread-sheets that enable monitoring of compliance with statutory timeframes for responding to requests. Quarterly FOI Performance reports:

- Provide details of the response timeframes,
- The directorates responsible for the timeframe failures.

A further analysis of the delayed responses is now being produced that highlights the units within the directorates. The quarterly performance report also contains details of complaints that have been received and the outcome of the complaint. Analysis of the spread-sheet used for monitoring confirmed that the information reported in the quarterly performance reports agreed with the details contained in the monitoring spread-sheets.

12. Subject Access Requests and Exemptions for Information

12.1 The GLA has not designed a specific Data Subject Access Request Policy, but has incorporated the process that individuals are to follow to obtain access to their personal information in the Data Protection Policy. Principally, upon receipt of a request for information:

- A form is sent to the requestor asking for details of the information required, and
- The proof of identification required by GLA.

Although the GLA can in accordance with the Data Protection Act levy a charge of £10, it does not request payment for the information. The policy identifies that staff and members of the general public have the right to request access to the data that the GLA is holding in relation to them.

12.2 The GLA has a procedure in place to ensure that data subject access requests are processed within the agreed timeframes i.e. within 40 days of the request being made. A review of a sample of subject access requests that had been received during the current financial year confirmed that a response to the request was provided within the 40 day timeframe.

13 Information Governance Training and Awareness

13.1 Staff are provided with information governance awareness training during their induction and provided with details of the intranet links for data protection and freedom of information pages. The intranet provides staff with on-going awareness information and is updated on a regular basis with GLA specific information and with information obtained from the Information Commissioners website. In addition,

- The Business Manager has obtained an ISEB qualification in Data Protection,
- The Information Governance Manager has obtained an ISEB qualification in Freedom of Information and Data Protection.

13.2 We found the design of the provision of on-going awareness information to staff to be adequate in reducing the risk that staff knowledge of GLA and legislative requirements is not up to date and not adhered to.

RISK AND AUDIT ASSURANCE STATEMENT - DEFINITIONS

Assurance Level	Assurance	Criteria
1	**Full** There is particularly effective management of key risks and business objectives are being achieved.	There is a sound framework of control operating effectively to achieve business objectives.
2	**Substantial** Key risks are being managed effectively, however some controls need to be improved to ensure business objectives are met.	The framework of control is adequate and controls to mitigate key risks are generally operating effectively.
3	**Limited** Some improvement is required to address key risks before business objectives can be met.	A number of controls to mitigate key risks are not operating effectively.
4	**No** Significant improvement is required to address key risks before business objectives can be met.	The control framework is inadequate and controls in place are not operating effectively to mitigate key risks. The business area is open to abuse, significant error or loss and/or misappropriation.

Definitions of Risk Ratings

Priority	Categories recommendations according to their level of priority.
1	Critical risk issues for the attention of senior management to address control weakness that could have significant impact upon not only the system, function or process objectives, but also the achievement of the organisation's objectives in relation to: • The efficient and effective use of resources • The safeguarding of assets • The preparation of reliable financial and operational information • Compliance with laws and regulations.
2	Major risk issues for the attention of senior management to address control weaknesses that has or is likely to have a significant impact upon the achievement of key system, function or process objectives. This weakness, whilst high impact for the system, function or process does not have a significant impact on the achievement of the overall organisational objectives.
3	Other recommendations for local management action to address risk and control weakness that has a low impact on the achievement of the key system, function or process objectives ; or this weakness has exposed the system, function or process to a key risk, however the likelihood is this risk occurring is low.
4	Minor matters need to address risk and control weakness that does not impact upon the achievement of key system, function or process or process objectives; however implementation of the recommendation would improve overall control.

Ref.	Risk and Recommendation	Priority	Agreed Action	Accepted	Responsibility	Target Date
7.3	A lack of procedures for informing the Data Protection Officer of any new or changes to existing systems or methods of processing personal data (electronic or manual) increases the risk that the GLA may not be able to ensure that they are processing data in accordance with their notification to the Information Commissioner or legislative requirements. A process needs to be designed for ensuring the Data Protection Officer is informed of any changes to the way that personal data is processed, in accordance with the Information Commissioner and related legislative requirements.	3	Amended procedures which have previously been used when updating our notification and forms will be made available on our intranet page which will allow staff to inform the DPO of any changes to the processing of personal data.	Yes	IT Business Manager	End of July 2012
7.4	The GLA may be censured by the Information Commissioner for not notifying that it is using CCTV. The GLA needs to notify the Information Commissioner's Office that CCTV systems are operating in premises for prevention and detection of crime.	3	Since the Information Management (IM) audit commenced the notification department at the ICO's offices have been informed via email that we operate CCTV for the purpose of crime prevention and prosecution of offenders	Yes	IT Business Manager	End of June 2012
7.5	A lack of data audit increases that risk that the notification to the Information Commissioner may not reflect all	3	The DPO agrees to carry out an annual review of the processing of personal data to ensure that our notification reflects all processing taking	Yes	IT Business Manager	Nov 2012

Ref.	Risk and Recommendation	Priority	Agreed Action	Accepted	Responsibility	Target Date
	processing that are taking place within the Association. However; the periodic requests by the Data Protection Officer for information regarding the processing of personal data reduces this risk. Annual reviews should be undertaken to ensure that the GLA complies with the requirements of Data Protection.		place and ensure that the GLA response effectively to subject access requests.			
7.6	The design of the document retention guidelines was found to be adequate in identifying the retention periods for key data that is held by the GLA. However; as the schedule is dated 2004 it should be reviewed to ensure that it is accurate and reflects the latest data retention requirements as there is a risk that data could be retained for longer than necessary in contravention of the fifth principle of the Data Protection Act 1998	4	Since the Information Management audit commenced, the GLA's records retention schedule has been reviewed and updated (see attached). A new version has now been approved by senior management and published on the GLA Intranet for staff use.	Yes	Information Governance Manager	Complete
8.1	The lack of implementation of the Government Protective Marking Scheme model increases the risk that sensitive information that should not be disclosed is inadvertently passed on, included as an email attachment or information received from a stakeholder is incorrectly handled due to staff not being aware of the correct processes for handling protectively marked material.	3	The GLA's Governance Steering Group (comprising the Head of Paid Service, Director of Resources, Director of Secretariat and the Monitoring Officer amongst others) will be asked to reconsider whether it is in the best interests of the GLA to adopt a protective marking scheme such as that drafted in 2009.	Yes	Information Governance Manager	12 July 2012

Ref.	Risk and Recommendation	Priority	Agreed Action	Accepted	Responsibility	Target Date
	The GLA needs to reconsider the introduction of a Protective Marking Scheme.					
9.2	The failure to have documented a web cookies policy increases the risk that the legal requirements may not be implemented by end of May 2012. The Information Commissioner has already provided a one year grace period for implementation. This could lead to censure by the Information Commissioner or possible fine. The GLA website needs to be updated to comply with the EU privacy and electronic directive law.	2	Work has been underway to ensure that the GLA's website and use of cookies complies with the EU changes to the Privacy and Electronic Communication Regulations by the end of the Information Commissioner's grace period at the end of May 2012. Since the Information Management audit started, the GLA's interim Senior Digital Marketing Manager has conducted an audit to check what type of cookies the GLA's website uses and assessed how intrusive the GLA's use of cookies is. This work is now complete.	Yes	Information Governance Manager	Complete
9.3	The lack of records of data sharing protocols increases the risk that data could be shared that has not been approved for sharing resulting in adverse publicity for GLA and censure by the Information Commissioner. Data sharing protocols and agreements should be reviewed and made available to all users as necessary.	3	The DPO and the information governance team will make available advice and templates for data sharing agreements and will adapt the existing notification review forms to include details of any data sharing agreements.	Yes	IT Business Manager	November 2012