Audit, Risk & Assurance Committee

Date	30 January 2024
Report title	Information Governance Annual Report
Accountable Chief Executive	Laura Shoaf, Chief Executive
Accountable Employee	Gurmit Sangha, Data Protection Officer WMCA Email: gurmit.sangha@wmca.org.uk
Report has been considered by	N/a

Recommendation(s) for action or decision:

The Audit, Risk and Assurance Committee recommended to:

(1) Note and consider the key messages in the annual information governance update on the processing of information at WMCA.

(2) Provide comment and opinion on future information governance activity.

1. Purpose

This report seeks to provide the Audit, Risk and Assurance Committee sufficient information on the WMCA meeting its obligations under the UK General Data Protection Regulation, the Data Protection Act 2018, any other applicable law relating to the processing, privacy and/or use of Personal Data and the Freedom of Information Act 2000, highlighting:

- Key information governance activities undertaken during 2023.
- The most significant current and emerging Data Privacy information governance issues.
- The measures WMCA intends to implement during 2024 to improve and ensure we meet data protection compliance standards.

2. Background

Data protection legislation is designed to protect “personal data.” It regulates the processing of this data setting obligations on any organisation handling personal information (Information from which an individual can be identified).

WMCA must meet its statutory responsibilities effectively and protect the personal information it holds throughout its life cycle; from creation through storage; use, retention, archiving and deletion. Failure to meet the data protection regime can result in financial loss, regulatory fines, legal action, and reputational damage.

WMCA has since 2018 overseen data protection governance through the statutory post of Data Protection Officer which we are mandated to have in place by the Data Protection Act 2018.

3. Overview of key enhancements in 2023

3.1 Information Governance Structure:

WMCA has restructured its information governance regime during 2023 to strengthen this area of work.

- Resourcing for information governance has been increased from 2024 from one post to three posts. The extra resourcing will provide greater scope to monitor and improve compliance regimes, as well as being able to demonstrate assurance both internally and if required to an external regulator.
- All three information governance officers will report into the newly created Head of Audit and Information Governance post which has now been successfully recruited to. The move will bring a more audit based and analytical approach to obtaining assurance around information processing.

  The Head of Audit and Information Governance will also undertake responsibilities of Deputy Senior Information Risk Owner (Deputy - SIRO) for data processing carried out by WMCA. The SIRO (WMCA Chief Executive) is responsible for the overall ownership of WMCA’s information risk assurance and strategy. The Deputy SIRO will lead the ongoing assurance and monitoring activities of information governance.
- Establishment of a new Information Governance Group (IGG) in 2023 with new defined terms of reference and meeting bi-monthly. IGG will spearhead all work around improving information governance and compliance. Its forward plan for 2024 is set out within section 5 below.

3.2 Review of Information Governance policies:

During 2023 the following information governance policies were reviewed and amended to ensure they remain fit for purpose:

- Data Protection Policy
- Information Security Acceptable Use Policy
- Information Security Incident Reporting Policy
- Information Security Management Framework
- Information Security Policy
- Information Security Internet and Email Use Policy

First half of 2024 will include work on disseminating the content and requirements of the above policies across WMCA.

During 2024 we will also undertake an overhaul of the following policies:

- Information retention and disposal policy
- Security Incident Reporting Procedure
- AI Use Policy

3.3 Technical security:

As with all organisations the risk of criminal cyber activity remains significant. WMCA Digital and Data team implement a range of controls designed to prevent such activity. These controls have successfully detected and mitigated malicious activity and/or suspicious events. Additionally, the Digital and Data team has amongst other workstreams:

- Commenced a Cyber Remediation Plan.
- Improved position re: backup & restore.
- Undertaken penetration testing.
- Implemented 2 factor authentication on all accounts.
- Reviewed all WMCA user accounts and closed inactive accounts.
- Reviewed security tools to ensure that we are maximizing their application them.
- Reviewed software to ensure it up to date.

The work undertaken by the Digital & Data team around the technical protection of information provides assurance. However globally 2023 highlighted the importance of WMCA avoiding complacency. The message from the Information Regulator is that those tasked with monitoring risk and assurance should continue to focus on and analyse their organisations activity in this area to maintain the best possible risk mitigation. The risk assurance challenge magnifies with the ever-increasing reliance on digital technology to support business activities.

3.4 Cyber Essentials.

Remedial work to obtain Cyber Essentials accreditation continued during 2023. The continued absence of this accreditation remains an ongoing issue, and the Committee will be aware of the history of this matter. Accreditation will be achieved in 2024 and importantly the Data Protection Officer will stress the need for the Digital and Data Team to maintain accreditation through active workstreams.

3.5 Bring Your Own Device (BYOD)

BYOD involves the access of WMCA data from remote devices (Mobile phones, tablets, etc). It has been a longstanding area of concern having grown organically without any controlled governance. The process of seeking Cyber Essentials has expediated an implementation of BYOD governance. This will include the introduction of a BYOD policy that will enable a level of compliance to be applied in this area. External advice and support has been obtained in this area during 2023. It is anticipated that a formal policy will be introduced in 2024.

WMCA Information Governance Group will monitor BYOD to ensure best practice is followed in this area.

3.6 Information Security Incidents

An information security incident refers to the actual or potential loss, destruction, or unauthorised access to information. We are required by data protection legislation to report to the Office of the Information Commissioner (ICO) the most serious incidents.

The numbers of such incidents reported in 2023 remain low.

No incidents required reporting to the ICO.

We are currently reviewing our incident reporting mechanisms and awareness of reporting across the organisation as part of a wider business continuity review. The aim would be to introduce more robust reporting and empower staff across WMCA to be proactive when a breach may occur, so that we can deal with the issue, but also learn from it as part of continuous improvement.

Once steps to improve reporting are put in place, we anticipate an increase in reported incidents at the lower risk/impact scale over 2024.

3.7 Communications and Information Handling Awareness Raising

The Office of the Information Commissioner has reflected that employees are often the weakest link in terms of causing incidents. WMCA reported information security incidents also reflects this, and technical measures will never be totally effective especially given the increased sophistication of cyber-attacks including phishing. The move to more home working has increased the risk of this and so employee awareness is more important than ever. This is generally achieved via staff training together with other forms of communication to improve awareness.

We continue to raise awareness with staff and work with WMCA Learning and Development team to deliver the most effective information handling messages. During 2024 we will focus on awareness raising in selected areas rather than a broad sweep. This will help mitigate higher risk areas and improve maturity in those areas.

3.8 General

The ongoing programme of implementing privacy by design, maintaining data processing transparency, contractual data protection legalities, providing advice/assistance across WMCA on the processing of information, and fulfilling the requirements of data protection legislation have been maintained since the last Information Governance report before the Committee.

3.9 Freedom of Information and Subject Access

During 2023 WMCA received 152 Freedom of Information requests and 5 Subject Access Requests for personal data. 93% of requests were responded within the statutory time limit.

2 requestors appealed to the Information Commissioner on the handling of their requests. Both matters were successfully resolved.

4. Emerging Data Privacy, Cyber Security, and Information Governance (IG) issues

4.1 Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS Standard is an information security standard designed to reduce payment card fraud by increasing security controls around cardholder data. It aims to ensure credit

card transactions processed by an organisation are safe and there are safeguards against any potential breaches. WMCA processes PCA DSS data in several areas.

A new version of the PCI DSS standard (version 4.0) goes into effect on 31 **March 2024,** and has 63 new requirements. WMCA will ensure any new requirements of the standard are met. However, PCI DSS compliance has not been subject to a formal audit at WMCA, and this may be something the Committee may wish WMCA to address.

4.2 WMCA Information Governance and security Frameworks

A key principle of the UK GDPR is that we must process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle of data protection legislation.

To address the above in 2021 WMCA committed to attaining compliance and measuring against the levels mandated by HMG Security Policy Framework (HMG SPF) and Government Security standard 007. Unlike for example the ISO 27001 information standard HMG SPF does not require a formal accreditation or certification process but sets out workstreams to meet the principle.

There is a view within WMCA that the above is not the most appropriate standard for WMCA to measure itself against.

WMCA information Governance Group will seek to firstly find a consensus on the most appropriate standard to measure information security and governance against. Secondly the Group will ensure that it is universally adopted throughout the organisation and there is a more robust review of operations against the standard(s) adopted. The appointment of the Head of Audit and Information Governance will provide gravitas to this activity.

4.3 Information Asset Registers and Information Asset Owners

The role of an Information Asset Owner (IAO) is to oversee the information assets (information held and processed) within their business area. They play a key role in fostering good information handling. An effective IAO should know:

- What information their team/department holds, what information is transferred in or out of it and what systems it links to.
- Know who has access and why and ensure that their use is monitored.
- Understand and address risks to the asset.
- Ensure the asset is fully used for its intended purpose or for the individual it relates to, including responding to access requests.

Information Asset Registers record the information held and how it is processed within the team/department. Additionally, they address a fundamental component of the UK GDPR (Article 30) that organisations to maintain detailed documentation of the processing activities it undertakes in relation to personal data.

We recognise there is some work to do be done in this area. During 2024 we will be reviewing the nomination of Information Asset Owners, their understanding of the role, and revisiting our approach to managing information assets.

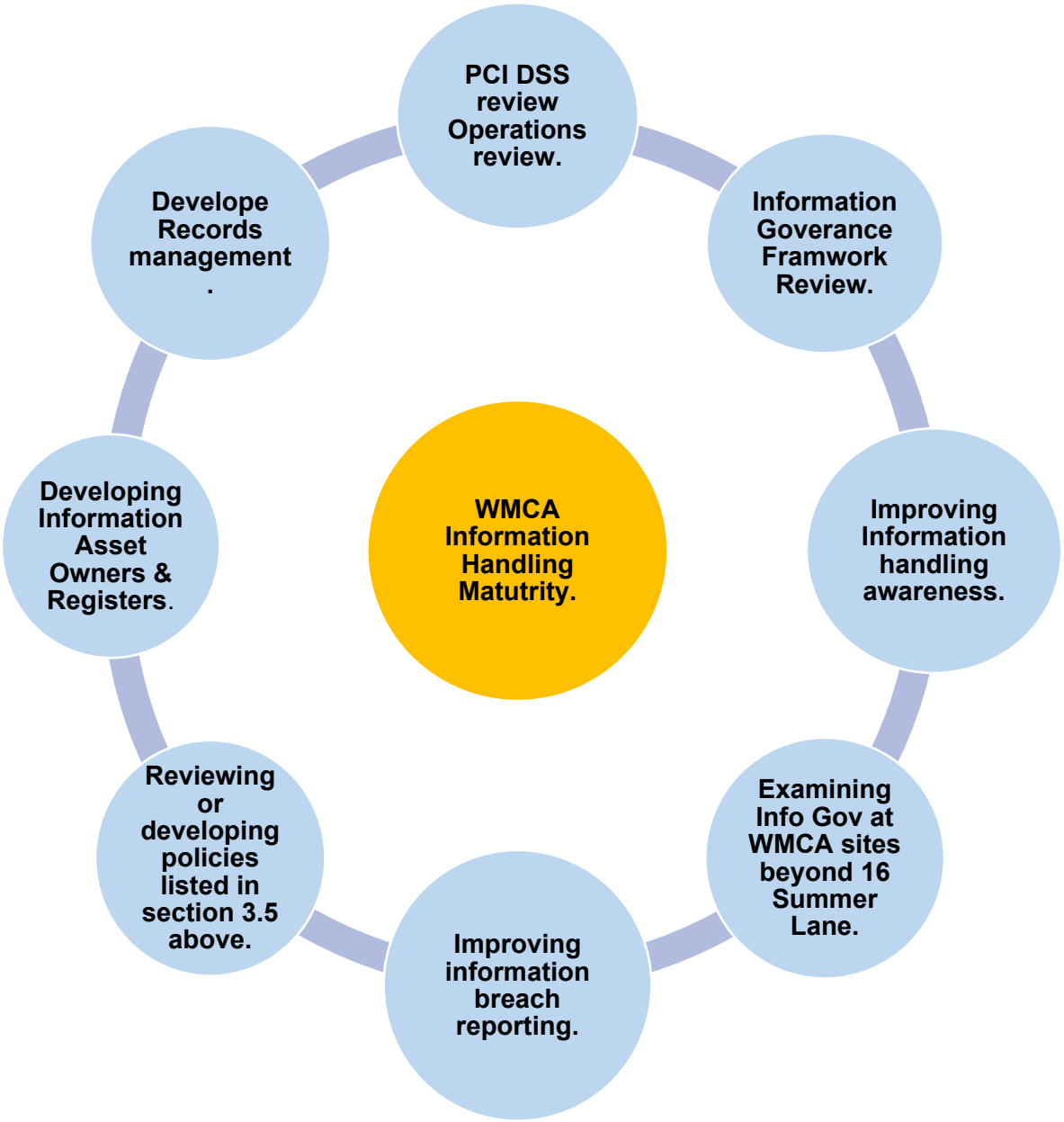
4.4 Records Management

Records management (the storage, naming and classification of documents) at WMCA operates predominantly at a local departmental/team level. Organisationally we provide a lower strategic lead in this area than other public bodies. Whilst this may have been

appropriate at formation of the Authority as our work has expanded through devolution from a transport authority to other areas of responsibility, greater strategic control may be needed. We will be undertaking a review of this area which will aim to ensure accurate, accessible, and protected information is retained.

5. 2024 Information Governance forward plan

The following diagram sets out the activity plan for the Information Governance Group during 2024. This work will look to strengthen WMCA maturity in the handling of personal information and thereby all other data.



6. Conclusion

The matters raised in this report should provide the Committee with assurance that WMCA understands the information risks that it faces and has in place and/or is developing processes and procedures to effectively manage Information Risk. Several key deliverables have been progressed over the last 12 months to develop a more robust approach to the effective management of Information Risk. The work planned for the coming 12 months should provide the Committee with additional assurance that there are appropriate plans in place to further embed key policies, procedures, and best practice.

7. Financial Implications

N/a

8. Legal Implications

N/a

9. Single Assurance Framework Implications

N/a

10. Equalities Implications

N/a

11. Inclusive Growth Implications

N/a

12. Geographical Area of Report's Implications

N/a

13. Other Implications

N/a

14. Schedule of Background Papers

N/a