Committee(s): Audit and Risk Management Information Systems Sub Committee	Date(s): 9th September 22nd September
Subject: Information Security and Governance	**Public**
Report of: Chamberlain	**For Information**

Summary

This report is in response to the actions from the minutes of the May Committee meeting of the Audit and Risk Committee and to provide a status update in relation to information security and governance.

Recommendation(s)

Members are asked to:

- Note the report

Main Report

Background

This report is designed to provide a response and update to mitigation of information security and governance risk (SR16) and further developments in this area:

- Update on current position: number of breaches
- Risk mitigation to date: training, communications, engagement
- Development of the IMGB (structure, changes, future approach and action plan)

Current Position and actions from last report

The following provides an outline of the current position and actions from the last report:

1. **Security Breaches:** There have been 2 breaches of information since the last report (May 2014). Both breaches were reported to the Information Officer through the correct course of action and neither were considered to be of a nature that they should be reported to the Information Commissioner.

    a. **Culture, Heritage and Libraries / Town Clerk's Department: 4/6/14** A Committee report was published on website containing: personal contact information of a third party. After notification the information was removed from the website. After investigation, it was concluded that the information was available elsewhere on the web, however we published a mobile contact number in error.

Action: Arranged for the following action: staff involved were reminded to be vigilant when handling personal information and asked to re-complete the DP e-learning package.

b. **GSMD:** 10/6/2014
Personal information of a current student was mistakenly added to an email sent to a rejected student. The information consisted of the current student's name and course information, and general reference to health issues, but the health issues were not specified.

Action: An apology was issued to data subject, i.e. the current student); the unintended recipient confirmed the email was deleted; staff involved were reminded to be vigilant when handling personal information and asked to re-complete the DP e-learning package.

2. **Mitigating Actions to avoid security breaches**

a. **Training:**

i. 123 staff have attended engagement presentations in Data Protection to date in 2014.

ii. 57 staff have completed Protecting information level 1, 2 or 3 relating to their role in 2014

iii. 35 staff completed Data Security training in 2014 so far.

b. **Communication and awareness:** there has been further communication to all City staff through the following means with respect to handling information with emphasis on Data Protection, breaches of which can incur the biggest penalty for the City Corporation.

i. Email infographic sent to all staff from the Deputy Town Clerk 5 August 2014 and used as office posters for the next two weeks (see appendix 1)

ii. Email about building security sent to all staff on 31 July 2014

iii. Email about 'being aware of 'phishing' sent to all staff on 19 August 2014 with links to further information on Data Security training

iv. Communication of 'one stop shop' diagram to reporting information security incidents – paper based, personal information, loss or theft of devices and building security published on the intranet. See appendix 2.

c. Improvement in auditing the Mitigation of Risk

i. Data Protection compliance checks through the AIN (access to information) representatives as a pilot process commenced in November 2013. This involves working with AIN reps to check local security arrangements for physical security of items (physical security of information through storage and transportation, clear desk policy for those working with personal/sensitive data). This will be rolled out further and broadened over time to fully cover retention of personal data.

ii. Clarity in the reporting process: an agreed 'back office' incident escalation process is outlined in Appendix 4.

iii. In time for Learning and Development week in October 2014, the new Learning Management System will be rolled out across the City Corporation. This presents the opportunity to promote the most up to date information management courses to staff and target those staff who handle personal or sensitive information and track their course completion more fully and present completion statistics back to the Board.

Development of the IMGB

1. Terms of Reference:

    a. The IMGB (Information Management Governance Board) is now a **strategic board only**.
    b. The purpose of the board is to decide on the most pressing areas of concern in relation to IMG (information management and governance) and identify the key business areas and experts to collaborate with in addressing IMG issues.
    c. It will then recommend interventions such as workshops, policy development, communication and training in relation to best practice in the field of information governance and management where applicable – corporately and departmentally.

After careful consideration of the performance of the previous IMGB, this approach was agreed by both the SIRO and Chair (listed in Appendix 1). The ambition is to develop effectiveness and efficiency in information governance and management through a fresh approach, using organisational expertise to best effect and reduce bureaucracy. An outline of Board Members and planned activity for Autumn 2014 is included in Appendix 1.

Conclusion

This report has outlined progress since the last report submitted in May 2014 and sets out the planned course of action going forward.

Appendices

- Appendix 1: IMGB: Structure and engagement plan
- Appendix 2: Example of staff communications since May 2014
- Appendix 3: Flow diagram for staff information of incident reporting for ‘information breaches’ in relation to sensitive, hardcopy/online, and building security.
- Appendix 4: Flow diagram of incident escalation/decision in the event of a breach.

Graham Bell
Chief Information Officer and SIRO (Senior Information Risk Officer)

T: 0207 332 1307
E: graham.bell@cityoflondon.gov.uk

Appendix 1: IMGB membership and action plan

IMGB: Membership

- Director of the Built Environment (*chair*)
- Chief Information Officer (*SIRO, or Senior Information Risk Officer*)
- Head of Corporate Performance and Development, Town Clerks
- Strategy, Research and Information Lead, Chamberlain's

→

- Summit Group
- Chief Officer Group

Seek corporate decision (policy refresh etc)

Consult with CoI Information Experts through workshops etc.

Head of Corporate Performance is line manager to Information Officers

Expert	**Topic**
Archivists (London Metropolitan Archives)	Record management
Technical Architects/IS and Agilisys	Data Security, system decommissioning, data retention and disposal
Committee and Member Services	Member training and education, information handling and access
VIP team (IS)	
Caldicott Guardian (Children and Community Services)	Handling sensitive and confidential information/ protective marking
Audit and Risk Team	Record retention
Information Officer x 2	DP/FOI – record retention Handling sensitive information FOI requests
Lawyers (Comptroller and City Solicitors)	Record management

Action Plan: Autumn/Winter 2014

Activity	Action	Owner	Completion Date
Protective Marking Information classification awareness in line with 2014 legislation	Direct approach to areas required to classify sensitive information. Work with business areas to identity areas this applies to and assist them in achieving this	Strategy, Research and Information Lead, Chamberlains	September 2014
Ensure robust online security policy and plans are in place.	Refresh and agree information security policy for online systems. Promote online security and training	Strategy, Research and Information Lead, Chamberlains	October 2014
Clear desk policy for those dealing with sensitive information	Work with departments and Chief Officers to identify those dealing with sensitive information to encourage and sponsor clear desk policy in key areas. Assess success factors of this.	Strategy, Research and Information Lead, Chamberlains	October-December 2014
Audit compliance of Data Protection Act	Work with AIN representatives to develop and expand audit of areas to assess DP compliance. Explore and understand mechanism for secure transportation of non-public committee reports. question	Information Officers, Town Clerks	Winter 2014
Promote new Civil Service Information Governance and security modules	Rollout and promote 4 new training modules that include cyber security awareness: • Course for General Users/all staff • Course of Information Asset Owners (IAOs) • Course for Senior Information Risk Owners • Course for non-executive director/Board Members	Strategy, Research and Information Lead in partnership with HR and Information Officers.	October 2014

Appendix 2: Example of communications to staff:

Data Protection e-Flyer and Screensaver: Summer 2014

Data Protection

Are you data aware?

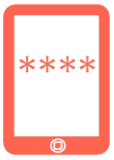
Please take note of the following good practice to avoid breaching the Data Protection Act and compromising people's personal information, which could result in enforcement action against the City of London. A more detailed version of this guidance is available on the **policy pages of colnet**.

Emailing personal information?
- Use the 'bcc' for multiple recipients
- Don't include personal information within an email chain
- Don't unnecessarily disclose names and email addresses of colleagues in the 'cc' option.

Remember - the IS Division have software to assist managing large mailshots and circulation lists: Listserve

Manual files containing personal information should always be kept secure, for example, in a locked cupboard

Ask your manager before removing personal information from the office.
- Take extra care when using public transport
- Don't leave laptops, files etc. visible in a car!
- Consider the use of secure pouches outside the office.



Portable devices must be kept secure, encrypted and password protected. Further advice on their secure use is available from the IS Division.

Do not keep personal information for longer than necessary. Ensure all personal information is disposed of securely.

When you are away from your desk lock your PC and do not leave personal information displayed on your desk.

Take care when using printers, photocopiers and network drives. Collect your information promptly, and do not leave any personal information on shared network drives (e.g. W Drive).

Passwords used to access personal information must always be kept secure and not shared.

Do not post personal information online, including when using social media, unless you know you are allowed to do so. This includes written information and photos/videos.

If using Cloud computing solutions to store, access or share personal information, ensure that there is sufficient security in place, and that all appropriate guidance is followed. Further advice on the secure use of Cloud computing solutions is available from the IS Division.

Avoid emailing and faxing personal information to recipients outside the organisation.
- If there is no alternative, ensure the recipient can confirm safe delivery
- Always take extra care when inputting the email address/fax number.
- If the personal information is particularly sensitive, consider using a secure email service (available through the IS Division).

If you find you can access personal information which you would not normally be permitted to access, please report it immediately and ensure your access is removed.

More information

There is a Data Protection e-learning module on the intranet. All employees who regularly access personal information should have gone through this (in accordance with the Employee Data Protection Policy). If you have not yet completed this please take some time now to do so.

It is essential that any breaches, or potential breaches, of the Data Protection Act are immediately reported to the **Town Clerk's Department** for a full investigation.

Most penalties issued by the Information Commissioner against public authorities for breaching the DPA have been in excess of £100,000

All enforcement cases are listed on the Information Commissioner's website and updated on our intranet pages

In some cases disciplinary action will need to be considered when breaches occur so do, please, be careful.

You can also find information here:

Employee Handbook
IS Guidelines
Access to Information representatives

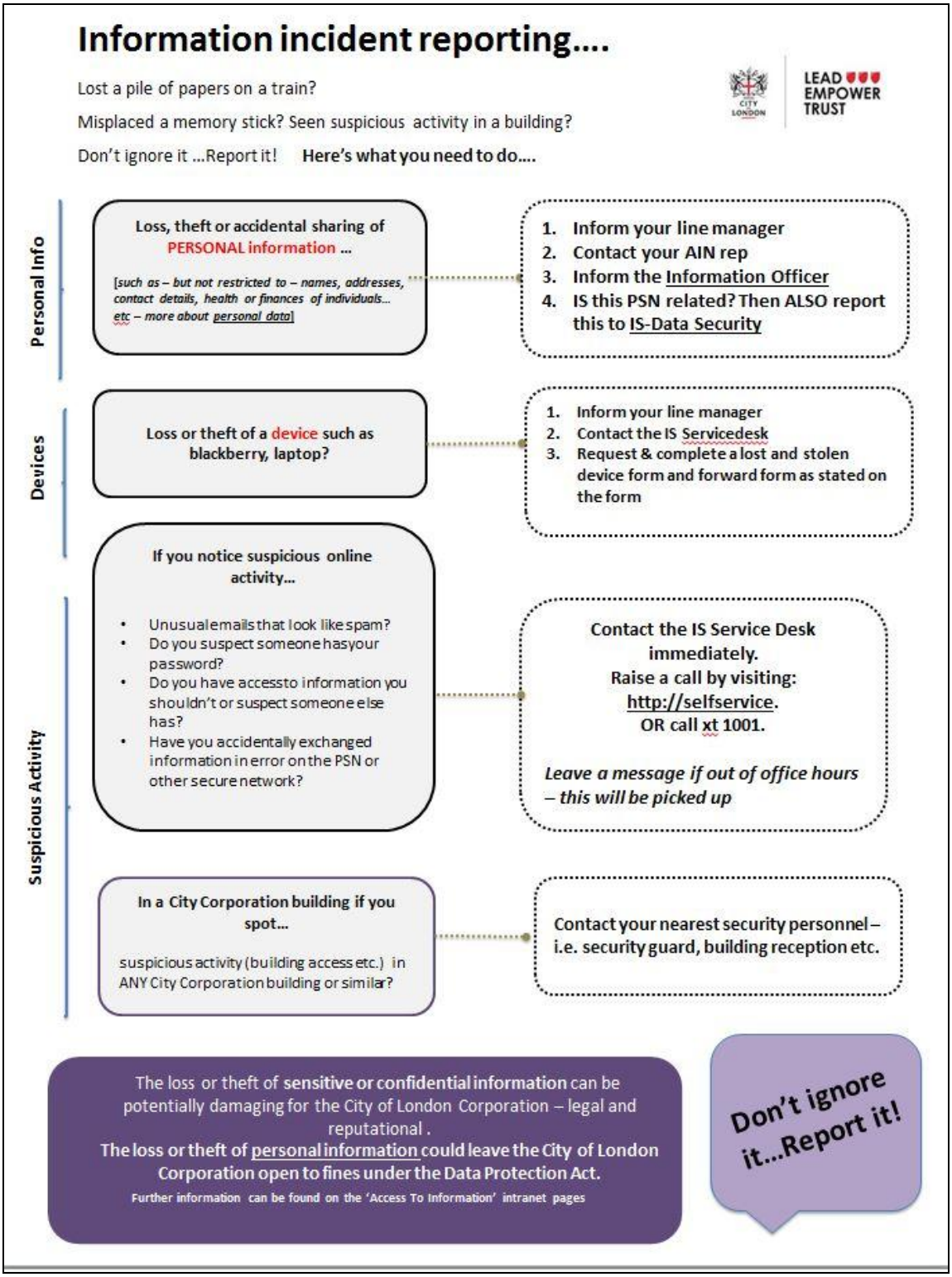
or contact

Information Officer (ext1209)
Assistant Information Officer (ext 3244)

Appendix 3:

Flow chart for Information Incident reporting:

Staff Information now available on intranet.



Appendix 4: Flow diagram of agreed escalation process structure (back office) once an information breach is recorded.