Committee(s)	Dated:
Summit Digital Services Sub Committee (DSSC)	23rd October 2019 1st November 2019
Subject: City of London Corporation Information Management Protective Marking	**Public**
Report of: Michael Cougher - Comptroller Peter Kane - Chamberlain	**Summit for Decision** **DSSC for Information**
Report authors: Sean Green – IT Director	

Summary

The Information Management (IM) Strategy was agreed by Summit in March 2019 and the Digital Services Sub-Committee in July 2019.

A Corporate risk was developed in March 2019 (see Appendix A below) that recognises the cultural and maturity issues the organisation faces currently with how we manage and support good information management curation and practices.

This paper presents the proposal to implement the national UK government protective marking schema in the organisation which, based on our current Microsoft licencing, will initially be manually applied however with future licence investment in 20/21 much of this can also be automated.

Recommendation(s)

Members are asked to:

- Note this report

Main Report

Background

1. In March 2018 Summit agreed the IM Strategy

2. The strategy seeks to transform IM capabilities (tools and skills) and culture (values and behaviours) across CoL and its partners so that accurate and timely information is routinely and effectively used as the basis for decisions and actions, thereby leading to better service outcomes.

3. When the IM Strategy was presented to Summit in March 2019 it was recognised that a corporate risk should be created (See Appendix A attached)

4. Protective Marking came into effect in April 2014 and describes how HM Government classifies information assets to ensure they are appropriately protected; support Public Sector business and the effective exploitation of

information; and meet the requirements of relevant legislation and international / bilateral agreements and obligations.

5. The Government's protective marking system is designed to help individuals determine, and indicate to others, the levels of protection required to help prevent the compromise of valuable or sensitive assets. The markings signal quickly and unambiguously, the value of an asset and the level of protection it needs.

6. It applies to all information that government collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners.

7. Everyone who works with government has a duty to respect the confidentiality and integrity of any HMG information and data that they access and is personally accountable for safeguarding assets in line with this policy.

8. HMG information assets may be classified into three types: OFFICIAL, SECRET and TOP SECRET. Each attracts a baseline set of security controls providing appropriate protection against typical threats. Additionally, ICT systems and services may require enhanced controls to manage the associated risks to aggregated data or to manage integrity and availability concerns.

9. The City of London Police applies security classification to all documents and emails internally and externally and has been in force for many years.

10. The use of the protective marking schemas in of itself can change the culture of how staff perceive and value the information that they manage on behalf of the organisation.

11. As we move to a more flexible model of remote working from smaller locations and home the potential for in appropriate handling and release of sensitive information could increase therefore the cultural impact that protective marking should bring about should be of benefit to CoL.

12. In summary implementing a simplified protective marking scheme improves our information security and supports the mitigating actions for CR29 (see Appendix A attached).

Proposal for Implementation of Protective Marking

13. It is proposed that CoL will apply protective labelling in a more pragmatic and practical way than the standard definitions provided by National Government with 4 labels and sub-categories that staff can choose that will be both be applied in the header, footer and watermark of the document

14. The proposed 3 labels chosen from a drop-down list are:

a. Suitable for Publication – Business data that is specifically prepared and approved for public consultation;
b. Official – All routine public sector business, operations and services should be treated as OFFICIAL;
c. Official Sensitive – A limited subset of OFFICIAL – information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media.

Note: Anything not marked will be considered as Non-business data for personal use only;

15. When Official Sensitive is chosen any email used to send the document will be encrypted. In addition, for this category there are 3 sub-categories that the member of staff will be offered from a drop-down list which are:
    a. Internal only – Will be encrypted so that it can only be opened with internal organisational email address or through whitelisted email addresses or domains;
    b. Commercial – Email or document can be externally sent and opened but will be encrypted.
    c. Personal Data – Contains personal data as defined by the data protection act. Can be sent externally but will be encrypted.

16. The process for applying labels to documents will be manual with a default to 'official'.

17. Alongside the small system changes there will be online training and an information management cultural change and communication campaign planned to run from 21st October – 15th November.

18. In the future when we upgrade our current Microsoft licences, we can automate the application of protective marking labels based on sensitive and personal data detected in documents using Artificial Intelligence rules.

Next Steps

19. Following launch of Protective Marking staff will be encouraged to undertake short training course and explanation of the benefits of the using the schema will be communicated through communication campaigns.

20. Feedback and use of Protective Marking will be sought 3 months after launch to evidence mitigation of the Corporate IM risk (see Appendix A below).

21. Further automation (using AI rules) and protection of sensitive data should be implemented in 2020 following proposed upgrades to the organisation's Microsoft Office licences.

IT Director
Chamberlain's Department

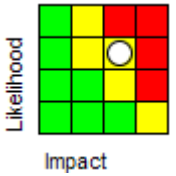
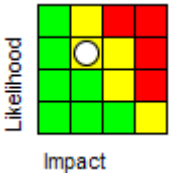
E: Sean.Green@cityoflondon.gov.uk

Appendix A – IM Corporate Risk

Appendix A – IM Risk - CR29

Report Author: Paul Dudley
Generated on: 16 August 2019

Rows are sorted by Risk Score

Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date	Current Risk score change indicator
CR29 Information Management	**Cause:** Lack of officer commitment and investment of the right resources into organisational information management systems and culture. **Event:** The City Corporation's IM Strategy (2018-2023) is not fully and effectively implemented **Effect:** • Not being able to use relevant information to draw insights and intelligence and support good decision-making • Vulnerability to personal data and other information rights breaches and non-compliance with possible ICO fines or other legal action • Waste of resources storing information beyond usefulness		**12**	The Information Management strategy has been agreed subject to a more detailed action plan and metrics to track performance. Progress is being made in developing a draft retention and disposal policy alongside reviewing roles to support good information management in the organisation and the business case for investment in tools required to help us manage and use our information more effectively. A draft Information Metrics model has been developed and discussed with the Information Management Board this now needs a final		**6**	30-Jun-2020	

08-Apr-2019 John Barradell				review with the Corporate Strategy and Performance team before being shared with Summit in September 2019 **09 Aug 2019**				Constant

Action no	Action description	Latest Note	Action owner	Latest Note Date	Due Date
CR29a	Ensure that CoL has the necessary awareness, tools and, skills to manage information effectively	Work with the Head of Communications to communicate/raise awareness the IM Strategy and Policies. Provide training in SharePoint in preparation for migrating the Shared drives. Implement protective marking and information classification in CoL. Sharepoint to become the Corporate document management solution. Launch of this to be October 2019	Sean Green	09-Aug-2019	31-Oct-2019
CR29b	Start the culture change by Integrating good information management practice into the Leadership and Management stand of the City of London Learning Academy	HR to work with the IT and the Corporate Strategy and Performance teams to identify the key skills required for good information management. HR to then develop the training to support this. HR to review where in HR policies and procedures this can be integrated. HR to Work with the senior leadership team to develop a plan and then deliver key messages and communications on the importance, relevance and benefits of good information management. Meeting held with HR who have agreed to support the development of training for the October launch	Chrissie Morgan	09-Aug-2019	31-Mar-2020
CR29c	Ensure that CoL's information estate is safe, relevant, accurate, reliable, used and trusted.	Implement and communicate relevant IM policies and IM Security.	Sean Green	09-Aug-2019	30-Sep-2019

		Develop and agree a Data Retention policy that links in with departmental retention schedules taking advice from the LMA. Draft Policy being reviewed by LMA to take back to SRG and Summit Draft records Mgt policy being presented to Info Gov Group at the end of July 19 and then to Summit in September 19			
CR29d	Ensure that CoL's derives real value and benefits from the use of information, data, analysis and modelling	IT to deliver the Business Intelligence Infrastructure to ensure that the Corporate Strategy and Performance team have the tools to develop business intelligence reports and analytics to support better decision making across CoL. Scope has been developed and is out for approval.	Sean Green; Kate Smith	09-Aug-2019	30-Aug-2019
CR29e	Ensure that CoL has the necessary checks, balances and oversight to ensure successful implementation of the IM Strategy	The Digital Services Task and Finish group to be established to provide governance and assurance that the strategy is being delivered. New IM Policies and compliance are already governed via the IM Governance Board. Meeting of this group booked has been delayed due to staff availability to attend. Now due to occur in September 2019	Sean Green	09-Aug-2019	30-Sep-2019
CR29f	Ensure officers can implement the data retention policy and data discovery requirements from GDPR	Put in place a new Data retention and discovery toolset to ensure we only retain and archive information in line with the agreed policy and retention schedule. Plan to use readily available MS tools and pilot the move of shared drives to MS Teams	Sean Green	09-Aug-2019	30-Nov-2019