Report to:	QSMTM 2023-24 Q4
Report by:	Helen Gardner-Swift, Head of Corporate Services (HOCS)
Meeting Date:	24 August 2023
Subject/ Title: (and VC no)	UK GDPR Update 2023-24 Q1 VC192537
Attached Papers (title and VC no)	None

Purpose of report

1. The purpose of this Committee Report (CR) is to update the Senior Management Team (SMT) on the organisational arrangements relating to the UK General Data Protection Regulation (UK GDPR) and data protection, including any relevant actions taken in Q3.

Recommendation and actions

2. I recommend:

   (i) the SMT notes the contents of this CR

   (ii) the SMT agrees the publication of the CR as set out in paragraph 42.

Executive summary

Background

Legislation

3. The DPA 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR) impose obligations on the processing of personal data held by the Scottish Information Commissioner (Commissioner) and have implications for every part of our organisation.

C5 Data Protection Policy and Handbook

4. This key document sets out how the Commissioner complies with the Data Protection Act 2018 (DPA) and the UK GDPR. The aim of the policy and the related procedures and guidance is to ensure that the Commissioner meets the requirements of the DPA 2018 and the UK GDPR. Relevant templates for members of staff are also in place.

Organisational responsibilities

5. The SMT has overall responsibility for the C5 Data Protection Policy and Handbook.

6. The SMT is responsible for ensuring the C5 Data Protection Policy and Handbook are followed and that staff competence is maintained and developed.

7. The HOCS is the Responsible Manager for the review and update of the C5 Data Protection Policy and Handbook, as necessary. The planned review of the document has been undertaken and no substantial changes, requiring SMT approval was required.

8. The HOCS monitors compliance with the C5 Data Protection Policy and Handbook, provides a quarterly update report to the SMT (this CR) and provides annual assurance to the Commissioner that the C5 Data Protection Policy and Handbook are being followed (this

assurance is provided as part of the assurance relating to the information and management of records).

9. The HOCS is the main point of contact with the DPO and keeps under review the matters upon which advice is sought from the DPO or when the DPO is notified of a data incident.

10. If a data incident takes place, the HOCS has overall responsibility for coordinating the Data Incident Management Plan (DIMP). In cases where there is unlikely to be a significant data incident, the FAM will coordinate the DIMP.

11. The Commissioner's Data Protection Notification is kept up to date by the FAM.

12. The GDPR Working Party (internal) was established in 2017 to oversee the implementation of the EU GDPR and DPA 2018 requirements and continues to provide advice and guidance on relevant data protection matters including the following:

    - the UK GDPR and DPA 2018 requirements
    - personal data processing
    - Privacy Notice updates
    - data incidents and data breaches
    - data protection impact assessments
    - data protection training

13. The GDPR Working Party is chaired by the HOCS and is made up of representatives from each business area – SMT, Enforcement, Corporate Services and Policy and Information. In the absence of the HOCS, the GDPR Working party is chaired by the HOE.

14. All staff are required to be aware of the provisions of the DPA 2018 and the UK GDPR and their impact on the work the Commissioner's office undertakes.

15. All staff must follow the guidance and procedures set out in the C5 Data Protection Policy and Handbook.

Data Protection Officer (DPO)

16. The SPCB provides a shared DPO service and the MOU for this was signed on 24 May 2018. Euan McCulloch, Deputy Head of Enforcement, has agreed to act as DPO if a conflict of interest arises in the operation of the shared service DPO.

17. The MOU has been reviewed and signed by the Commissioner. The MOU covered 2020-21 and 2021-22 and an update for the MOU for 2023-24 and going forward is awaited.

18. At the All Staff Meeting (ASM) on 27 April 2022, the DPO provided training to all staff on everyday data protection issues and challenges.

19. Robin Davidson, our DPO, is attended the SMT meeting on 27 April 2023.

DPO Network Group

20. The purpose of these meetings is to discuss general UK GDPR/data protection requirements and receive updates from the DPO. Myself and Liz Brown, the FAM, attend the bi-monthly meetings. An update on the matters discussed is provided to the GDPR Working Party. The SMT is also updated by email, when required.

21. Meetings of the DPO Network Group take place by MS Teams.

22. Our office premises re-opened in May 2022 and hybrid working is in place. We maintain operational output and guidance has been issued to staff covering:

    - security of information, including data protection
    - records management
    - data incident procedures

Q1 update

23. The following work is planned be carried out in 2023-24:

    - review of retention periods (project)
    - review of consent log (as required)
    - review of general policies and procedures (data protection update is considered where relevant)
    - ICO Children's Code (watching brief)
    - CJEU Decision – Special Category Data (watching brief and ICO guidance update)

Privacy Notice

24. The key document C5 Privacy Notice has been regularly reviewed in 2023-24.

Staff training

25. The annual all staff UK GDPR/data protection training/update is due to take place in Q3 and members of staff will be asked to complete online training modules provided on the ICO's website prior to this training.

26. Throughout 2023-24, there will be regular awareness raising activities focussing on reducing the risk of data protection incidents, for example, guidance provided at ASMs, emails from the FAM.

27. As part of their induction, all new members of staff are provided with general UK GDPR/data protection training (and, also, required to complete 2 of the online training modules provided on the ICO's website). More detailed training, using an external training provider, has been provided to all new members of staff in Q1.

Budget

28. There was no specific budget allocated for data protection/UK GDPR requirements in the approved budget for 2023-24.

Cyber resilience

29. Any element of a cyber security issue resulting in the loss of or harm to personal data is likely to be treated as a data breach.

30. Although not required to do so, the Commissioner follows the Scottish Government guidance on cyber security and is participating, as far as possible, in the Public Sector Action Plan as part of the Cyber Resilience Strategy issued by the Scottish Government. Appropriate action has been taken in response to early warning notices (Crew Notices) that have been sent to us by the Scottish Government's cyber resilience teams – Cyber Resilience Unit (CRU) the Scottish Cyber Coordination Centre (SC3).

31. The Commissioner was re-accredited with Cyber Essentials in March 2023 and with Cyber Essentials Plus in May 2023.

32. An on-going programme of cyber resilience training undertaken by all members of staff.

33. An internal audit relating to cyber resilience arrangements was undertaken in 2022-23 Q4.

Data Incidents

34. For 2023-24, the table below shows, for quarter 1, and to date, the number of data incidents and the action taken and also includes, for comparison, the relevant figures for 2022-23.

Data Incidents				
	2023-24			**2022-23**
	Number	DPO consulted	Reported to ICO	Number
Q1	1	Yes	No	1
Q2	2	Yes	No	2
Q3	0			3
Q4	0			2
Total	**3**			**8**

Risk impact

35. Compliance with UK GDPR and data protection requirements ensures that there are relevant and effective policies and procedures in place, including policies and procedures relating to information governance, data incidents, subject access, HR governance and privacy by design. In turn, this ensures that operational risks are mitigated as far as possible.

Equalities impact

36. There is no direct impact arising from this report. Equality and diversity matters will be considered in data protection requirements.

Privacy impact

37. There are no direct privacy implications arising from this report.

Resources impact

38. The staff resource required to enable the specific work in 2023-24 is met from within current resources.

Operational/ strategic plan impact

39. A project relating to the review of retention periods is included in the Operational Plan 2023-24.

Records management impact (including any key documents actions)

40. The planned review of the Key Document C5 Data Protection Policy and Handbook was undertaken in Q1.

Consultation and Communication

41. QSMTM Q1 minute.

Publication

42. This CR should be published in full.