Report to:	QSMTM 2022-23 Q4
Report by:	Helen Gardner-Swift, Head of Corporate Services (HOCS)
Meeting Date:	27 April 2023
Subject/ Title: (and VC no)	UK GDPR Update 2022-23 Q4 VC185726
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 45.

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 (approved in March 2021) 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 next planned review is due to be undertaken in 2023-24 (Q1/Q2).

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).

11. In cases where there is unlikely to be a significant data incident, the FAM will coordinate the DIMP.

12. The Commissioner's Data Protection Notification has been kept up to date by the FAM.

13. 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

14. 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.

15. 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.

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

Data Protection Officer (DPO)

17. 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.

18. 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 2022-23 and going forward is awaited.

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

20. Robin Davidson, our DPO, is attending the SMT meeting on 27 April 2023 (this meeting).

DPO Network Group

21. 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.

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

COVID-19 pandemic

23. Our priority as an organisation is to continue to provide services and guidance while safeguarding the health, safety and wellbeing of our members of staff.

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

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

Q4 update

25. The following work will be carried forward to 2023-24:

    - review of retention periods (project)
    - review of consent log
    - review of general policies and procedures (data protection update is considered where relevant)
    - ICO Children's Code (watching brief)
    - Rights Request Terminology (to be taken into account in review in DP Policy and Handbook)
    - CJEU Decision – Special Category Data (watching brief and ICO guidance update)

Privacy Notice

26. The key document C5 Privacy Notice has been regularly reviewed in 2022-23.

Staff training

27. The annual all staff UK GDPR/data protection training/update was undertaken in Q3 and members of staff completed 2 online training modules provided on the ICO's website prior to this training.

28. Throughout 2022-23, there have been regular awareness raising activities which focussed on reducing the risk of data protection incidents, for example, guidance provided at ASMs, emails from the FAM.

29. As part of their induction, all new members of staff have also been provided with general UK GDPR/data protection training (and required to complete 2 of the online training modules provided on the ICO's website). More detailed training, using an external training provider, will be provided to all new members of staff in 2023-24 Q1.

Budget

30. There was no specific budget allocated for data protection/UK GDPR requirements in the approved budget for 2022-23.

Cyber resilience

31. 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.

32. 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 Unit.

33. The Commissioner was re-accredited with Cyber Essentials in March 2023 and work on seeking Cyber Essentials Plus re-accreditation is being carried out in 2023-24 Q1.

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

35. The internal audit relating to cyber resilience arrangements was undertaken in Q4.

Data Incidents

36. There were no data incident in Q4.

2022-23

37. For 2022-23, the table below shows, for each quarter, the number of data incidents and the action taken and also includes, for comparison, the relevant figures for 2021-22.

Data Incidents				
	2022-23			**2021-22**
	Number	DPO consulted	Reported to ICO	Number
Q1	0	-	-	1
Q2	1	Yes	No	2
Q3	2	Yes	No	3
Q4	0	-	-	2
Total	**3**			**8**

Risk impact

38. 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

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

Privacy impact

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

Resources impact

41. The staff resource required to enable the specific work in 2022-23 is met from within current resources.

Operational/ strategic plan impact

42. A project relating to the review of retention periods was included in the Operational Plan 2022-23.

Records management impact (including any key documents actions)

43. As Responsible Manager, I due to the review of the Key Document C5 Data Protection Policy and Handbook in 2023-24 (Q1/Q2).

Consultation and Communication

44. QSMTM Q4 minute.

Publication

45. This CR should be published in full.