Report to:	QSMTM 2022-23 Q1
Report by:	Helen Gardner-Swift, Head of Corporate Services (HOCS)
Meeting Date:	27 October 2022
Subject/ Title: (and VC no)	UK GDPR Update 2022-23 Q2 VC176436
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 and any relevant actions taken in Q2.

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 44.

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 Data Protection Policy and Handbook.

6. The SMT is responsible for ensuring the 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 Data Protection Policy and Handbook as necessary. The next planned review is due to be carried out in March 2023.

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

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 FAM has responsibility for ensuring that the Commissioner's Data Protection Notification is kept up to date.

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:

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

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 I am awaiting an update for the MOU for 2022-23.

19. Robin Davidson, our DPO, attended a SMT meeting on 29 March 2022 and the All Staff Meeting (ASM) on 27 April 2022. At the ASM, the DPO provided training to all staff on everyday data protection issues and challenges.

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 currently take place by MS Teams.

COVID –19 pandemic

22. As a result of the impact of the COVID-19 pandemic, the following actions have been taken:

- the office premises re-opened on 3 May 2022
- following the gradual re-opening of the office premises on 3 May 2022, hybrid working is in place
- office security and IT security measures, including remote working measures, continue to be in place
- all members of staff are able to work remotely (with remote access to the office systems) using laptops and mobile phones provided by us and this includes the Commissioner and all members of the SMT
- guidance has been issued to staff covering:
    - security of information, including data protection
    - records management
    - data incident procedures
    - using MS Teams

2022-23 Q2

Specific work

23. The following specific work relating to data protection is due to be undertaken in 2022-23:

- review of retention periods (project)
- review of C5 Data Protection Policy and Handbook (planned review)
- review of consent log
- review of general policies and procedures (data protection update is considered where relevant)

Privacy Notice

24. The key document C5 Privacy Notice has been kept under review in Q2.

Staff training

25. Planning for this training has been undertaken in Q2 - the annual all staff UK GDPR/data protection training/update is due to take place in Q3.

26. All members of staff will be asked to complete the online data protection/UK GDPR training provided by the Scottish Parliament prior to the annual training/update.

27. Ad hoc awareness raising activities which focus on reducing the risk of data protection incidents continue, for example, emails from the FAM.

28. The GDPR Working Party is also considering the training modules provided by the Information Commissioner's Office.

Budget

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

Cyber resilience

30. 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.

31. 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.

32. The Commissioner was re-accredited with Cyber Essentials in December 2021 and Cyber Essentials Plus in March 2022.

33. Cyber resilience training being undertaken by all members of staff.

34. An internal audit on cyber resilience arrangements is due to take place in Q3.

Data Incidents

35. In Q1, there were no data incidents and there was one data incident in Q2 which did not need to be reported to the ICO. The DPO was consulted on this incident and the SMT approved the recommended actions.

36. The table below provides, for each quarter, the number of data incidents and the action taken and also includes details for 2021-22 so that a prior year comparison can be made.

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

Risk impact

37. 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

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

Privacy impact

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

Resources impact

40. The staff resource required to enable the specific work in 2022-23 will be met from within current resources.

Operational/ strategic plan impact

41. A project relating to the review of retention periods has been included in the Operational Plan 2022-23.

Records management impact (including any key documents actions)

42. As Responsible Manager, I will be reviewing the Key Document C5 Data Protection Policy and Handbook in 2022-23 Q4.

Consultation and Communication

43. QSMTM Q2 minute.

Publication

44. This CR should be published in full.