Report to:	QSMTM
Report by:	Helen Gardner-Swift, Head of Corporate Services (HOCS)
Meeting Date:	8 August 2019
Subject/ Title: (and VC no)	**GDPR Update to QSMTM** VC122101
Attached Papers (title and VC no)	None - the GDPR/DP Implementation Plan 2019-20 (VC116199) can be viewed in VC

Purpose of report

1. To update the Senior Management Team (SMT) on the implementation of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 requirements.

Recommendations

2. I recommend
   (i) the SMT notes the contents of this report
   (ii) the report is published in full save that the GDPR Implementation Plans 2017 – 18 (VC83922), 2018-19 (VC100858) And 2019 – 20 (VC116199) are not published for the reasons set out in paragraph 32.

Executive summary

Background

3. As you will be aware, data protection requirements changed from 25 May 2018 when the GDPR and Data Protection Act 2018 came into force.

4. In order to be able to ensure that the Commissioner complies with the relevant requirements, an implementation project was assigned to the HOCS for 2017-18. The project was was in two parts:

   (i) the development of an implementation plan – based on the 12 steps guidance issued by the ICO, this was developed and put in place in July 2017 (VC83922) and

   (ii) the delivery of an implementation plan –

5.
   (a) GDPR Implementation Plan 2018-19 (VC100858)
   (b) GDPR/DP Implementation Plan 2019-20 (VC116199) (agreed by QSMTM on 9 May 2019).

6. To assist with the delivery of the implementation plans, an internal GDPR Working Party was established in July 2017 and consists of myself (Chair), Margaret Keyse (SMT), Euan McCulloch (E), Lorraine Currie (P&I) and Liz Brown (CST). This group meets every 3 weeks.

7. Of the steps set out in the GDPR Implementation Plan 2019 -20, 52 have been completed and 21 are ongoing. The completed steps include:

- Personal data audit
- Identification of the types of processing of personal data and determining the legal basis for processing personal data
- Review of arrangements for the processing of personal data and update of arrangements
- Privacy notice
- Subject access procedures
- Consent – when required and recoding
- Data breach procedures (interim procedures)
- Staff training and update
- Review of supplier and services contracts
- Appointment of DPO
- Update of CR templates

8. The ongoing steps include

- update of general policies and procedures
- the revision of contracting guidance (interim guidance/procedures are in place)
- the revision of Data Protection Policy and Handbook (VC39909) (interim guidance is provided to staff)
- the approval of DPIA procedures and guidance
- the preparation of privacy by design guidance

9. From July 2019, the SPCB GDPR Working Party changed to the DPO Network Group, meets every two months and continues to be made up of Officeholders' representatives. The purpose of these meetings is to discuss general GDPR/data protection requirements and receive general updates from the DPO. I attend the bi-monthly meetings and update the GDPR Working Group on the matters discussed.

Data Protection Officer (DPO)

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

11. Myself and Euan met with our DPO 11 June 2019 for the annual review meeting and the following matters were discussed:

(i) DPO was updated on current and proposed projects which require/may require advice from the DPO re: related DPIAs.
(ii) Following the first year of operation of the MOU for the DPO Shared Service, the feedback has been positive and any further specific comments should be sent either to the DPO or to Janice Crerar (SPCB).
(iii) The DPO to attend a QSMTM meeting, possibly the Q3 meeting in late September 2019.
(iv) The DPO to meet with the GDPR Working Party, possibly before or after the above QSMTM
(v) The DPO to attend an ASM, possibly in October 2019 - this would provide an opportunity for the DPO to meet staff and provide a snippets training session.
(vi) The need for a cybersecurity group for officeholders - the DPO will discuss this with the SPCB
(vii) Recruitment and security vetting requirements and related data protection requirements

Staff training

12. All staff received a full day's GDPR training/update on 17 April 2018 on data protection reform and the new data protection rules and FOI.

13. Further staff training is being arranged for late September 2019/October 2019 – as there will be several new members of staff it would be better to hold this training in the Autumn rather than late Spring.

14. We have been provided with access to the online GDPR training provided in the Scottish Parliament and we are testing this at present. Once the test phase is completed, all staff will be asked to complete the training.

Costs

15. There is no specific budget allocated for GDPR/DP requirements in the 2019-20 budget.

Cyber resilience

16. 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.

17. Although not required to do so, SIC follows the Scottish Government guidance on cyber security and is participating in the Public Sector Action Plan as part of the Cyber Resilience Strategy issued by the Scottish Government.

18. The Commissioner is Cyber Essentials and Cyber Essential Plus accredited.

Data Incidents – Q1 2019-20

19. There were 3 data incidents in Q1, none of which required reporting to the DPO.

Risk impact

20. Risk 16 in the Operational Risk Register relates specifically to GDPR and Risks 10 (effective policies), 12 (HR governance), 13 (information governance) and 15 (subject access) are also relevant.

Equalities impact

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

Privacy impact

22. There are no direct privacy implications arising from this report. The relevant privacy requirements will be considered in revising data protection requirements so as to ensure the impact on privacy is minimised.

Resources impact

23. Additional staff resource is required as work on the GDPR/DP Implementation Plan 2019-20 continues.

Operational/ strategic plan impact

24. None at present.

Records management impact (including any key documents actions)

25. None at present.

Consultation and Communication

26. QSMTM minute, internal blog

Publication

27. I recommend that this committee report is published in full but that the GDPR Implementation Plan 2017-18, the GDPR Implementation Plan 2018-19 and the GDPR Implementation Plan 2019-20 are withheld on the basis that the exemption(s) in Sections 30(b)(ii) and 39(1) of the Freedom of Information (Scotland) Act 2002 would apply if an request were, at this stage, to be made for the information.