Report to:	QSMTM
Report by:	Helen Gardner-Swift, Head of Corporate Services (HOCS)
Meeting Date:	8 August 2018
Subject/ Title: (and VC no)	**GDPR Update** **VC105748**
Attached Papers (title and VC no)	None – the GDPR Implementation Plan 2018-19 (VC100858) 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
   - the SMT notes the contents of this report
   - the report is published in full save that the GDPR Implementation Plan 2018-19 (VC100858) is not published for the reasons set out in paragraph 29.

Executive summary

GDPR implementation

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 is in two parts:

   - 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

   - the delivery of the implementation plan – the GDPR Implementation Plan 2018-19 (VC100858).

5. To assist with the delivery of the implementation plan, 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 continues to meet (every 2/3 weeks).

6. Of the steps set out in the GDPR Implementation Plan 2018-19, 44 have been completed and 24 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
- Staff training and update
- Review of supplier and services contracts
- Appointment of DPO
- Update of CR templates

7. The ongoing steps include

- the revision of subject access guidance (interim guidance/procedures are in place)
- the revision of data breach guidance (interim guidance/procedures are in place)
- 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 variation of supplier and service contracts
- the preparation of privacy by design guidance

8. Myself and Euan McCulloch were also representatives on the Scottish Parliamentary Corporate Body (SPCB) GDPR Working party (monthly meetings) which enabled us to have an input into the actions being taken by Officeholders as regards GDPR preparation and compliance.

Data Protection Officer (DPO)

9. 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.

10. Myself and Euan met with our DPO on 26 July 2018 and provided information on our management structure, assurance and risk reporting, review of key documents with regard to data protection requirements, review of contracts with third party suppliers in relation to data protection, mandatory staff training on data protection, cyber resilience and the update of our data protection policy.

11. The DPO provided information regarding her role in relation to data breach requirements, agreed to share a data breach checklist and a list of Frequently Asked Questions (currently being developed by the DPO) and provided guidance on data protection impact assessment policy and procedures.

12. The DPO will be able to attend an annual QSMTM meeting to discuss data protection and attend any other strategy meeting where this would be helpful.

13. The SPCB GDPR Working Party has now changed into a DPO Network Group, meets every two months and continues to be made up of Officeholders' representatives. The first meeting took place on 18 July (myself and Euan attended). The purpose of these meetings will be to discuss general GDPR/data protection requirements and receive general updates from the DPO.

Staff training

14. All staff received GDPR training last year and on 17 January 2018 received update training on data protection reform and the new data protection rules and FOI. A full day's training was also provided to staff by Act Now! on 17 April 2018.

15. The SPCB has provided access to its online GDPR training and CST are currently testing this (to see how the training interacts with our systems) before it is rolled out to staff generally. The rollout is expected to happen in September/October 2018.

Costs

16. The following have been allocated in the 2018-19 budget:

DPO costs:	£10,000
GDPR implementation costs:	£5,000

17. As we now have a shared service DPO, the £10,000 allocated for this will be removed when the budget is next re-phased.

Cyber resilience

18. 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.

19. 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. The following actions are in place and/or will be undertaken in 2018/19:

- The Commissioner and myself have attended cyber security training sessions provided by the Scottish Government
- Additional staff training on cyber security will take place in 2018/19
- We receives regular newsletters and email alerts from the Cyber Resilience Unit and keep up to date on any cyber security issues in the public sector
- The Business Continuity Plan is being further reviewed to ensure that appropriate action is taken in respect of a cyber security issue
- a cyber incident management plan is in preparation

20. Having undertaken an assessment on 14 July 2018, the Commissioner is now Cyber Essentials accredited (we attained this well in advance of the Scottish Government deadline of 31 October 2018). An assessment for Cyber Essential Plus accreditation will be carried out in the next 2-3 months.

Risk impact

21. 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.

22. The residual risk assessment and severity tolerance level of 12 remains appropriate at the present time.

Equalities impact

23. Equality and diversity will be considered in revising data protection requirements so as to seek to ensure that no one is unlawfully discriminated against.

Resources impact

24. Additional staff resource is required as work on the GDPR implementation plan continues.

25. There may also be additional costs in seeking to vary existing contracts with service suppliers but no specific costs have been identified to date.

Operational/ strategic plan impact

26. None at present.

Records management impact (including any key documents actions)

27. None at present.

Consultation and Communication

28. QSMTM minute, internal blog

Publication

29. I recommend that this committee report is published in full but that the GDPR Implementation Plan 2018-19 is 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.