Report to:	QSMTM
Report by:	Helen Gardner-Swift
Meeting Date:	25 April 2018
Subject/ Title: (and VC no)	**GDPR Update** **VC101275**
Attached Papers (title and VC no)	GDPR Implementation Plan 2018-19 VC100858

Purpose of report

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

Recommendation and actions

2. I recommend
   (i) the SMT notes the contents of this report
   (ii) the SMT notes the GDPR Implementation Plan 2018-19 and the actions to be taken
   (iii) this report is published in full save that the GDPR Implementation Plan 2018-19 is not published

Executive summary

GDPR implementation

3. As you will be aware, data protection requirements are changing from 25 May 2018 when the new GDPR comes into force and the Data Protection (DP) Bill is due to come into force.

4. In order to be able to ensure that the SIC complies with the new requirements, an implementation project was assigned to the HOCS for 2017-18. This project has continued into 2018-19 and the GDPR Implementation Plan 2018-19 is attached.

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).

6. As we are approaching the implementation deadline, the GDPR Working Party meets every week. In addition to considering the GDPR Implementation Plan 2018-19 and the preparations/actions needed to ensure that SIC will comply with the GDPR and the DP Bill, the Working Party also takes account of the progress of the Data Protection Bill and the latest guidance from the Article 29 Working Party and the ICO.

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

Training

8. All staff received GDPR training in 2017 and on 17 January 2018 received some update training on the following:

- Data Protection Reform: Can we have the Bill please: provided by David Freeland, ICO's office (VC97644)
- The new data protection rules and FOI: provided by Margaret Keyse, Head of Enforcement (VC 97528)

9. Further GDPR training for all staff took place on 17 April 2018. The training was very useful and well received.

Data Protection Officer (DPO)

10. We are a public authority and, under the GDPR, are required to appoint a DPO. The DPO's minimum tasks are defined in Article 39 of the GDPR and include:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

11. The GDPR does not specify the precise credentials a DPO is expected to have but it does require that they should have professional experience and knowledge of data protection law - this should be proportionate to the type of processing we carry out, taking into consideration the level of protection the personal data requires.

12. As regards the appointment of a DPO, we must ensure that:

- the DPO reports to the highest management level, that is the SMT; and
- the DPO operates independently and is not dismissed or penalised for performing their task; and
- adequate resources are provided to enable the DPO to meet their GDPR obligations.

13. The role of the DPO can be allocated to an employee as long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests. The role of the DPO can also be contracted out externally. A single DPO can also be appointed to act for a group of public authorities, taking into account their structure and size.

14. The SPCB has put forward a shared service proposal for a DPO for Officeholders and we have provided comments on the draft MOU and are awaiting a response from the SPCB.

15. In the event that we enter into the proposed MOU and, subsequently, there is a conflict of interest which means that the SPCB DPO cannot act for the SIC, it is anticipated that a Deputy Head of Enforcement will act as a DPO (only in in these circumstances).

Budget

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

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

Risk impact

17. 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

18. Equality and diversity will be considered in revising data protection requirements so as to seek to ensure that all relevant equalities issues are taken into account.

Resources impact

19. Additional staff resource is required as work on the GDPR Implementation Plan 2018-19 progresses.

20. 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

21. None at present.

Records management impact (including any key documents actions)

22. None at present but a number of policies and procedures will need to be amended.

Consultation and Communication

23. QSMTM minute, staff blog re: updates from the GDPR Working Party

Publication

24. I recommend that this committee report is published in full but that the GDPR Implementation Plan 2018-19 is not published.