

Report to:	QSMTM
Report by:	Helen Gardner-Swift
Meeting Date:	1 June 2018
Subject/ Title: (and VC no)	GDPR Update VC103002
Attached Papers (title and VC no)	The GDPR Implementation Plan 2018-19 VC100858

Purpose of report

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

Recommendations

- 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 22.

Executive summary

GDPR implementation

- As you will be aware, data protection requirements changed from 25 May 2018 when the GDPR and Data Protection Act 2018 came into force.
- In order to be able to ensure that the SIC 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).
- 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).
- Of the steps set out in the GDPR Implementation Plan 2018-19, 42 have been completed and 26 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
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 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.

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 interests arises in the operation of the shared service DPO.

Staff training

10. All staff received GDPR training last year and on 17 January 2018 received update training on the 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.
11. 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.

Costs

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

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

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

Risk impact

14. 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.
15. The residual risk assessment and severity tolerance level of 12 remains appropriate at the present time.

Equalities impact

16. 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

17. Additional staff resource is required as work on the GDPR implementation plan continues.
18. 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

19. None at present.

Records management impact (including any key documents actions)

20. None at present.

Consultation and Communication

21. QSMTM minute, internal blog

Publication

22. 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.