

Report to:	QSMTM Q4
Report by:	Helen Gardner-Swift, Head of Corporate Services (HOCS)
Meeting Date:	12 May 2021
Subject/ Title: (and VC no)	Information and Records Management – Information and Records Management Report 2020-21 and Assurance VC149962
Attached Papers (title and VC no)	None

Purpose of report

1. To present the Information and Records Management Report 2020-21 (set out in the Appendix) (IRM Report 2020-21) and the assurance report as required by the Key Document C1 Governance Reporting Arrangements (GRA).

Recommendation and actions

2. The following is recommended
 - (i) the Senior Management Team (SMT) note this Committee Report (CR), the IRM Report 2020-21 and the assurance provided
 - (ii) the CR and the IRM Report 2020-21 are published in accordance with the details set out in paragraph 15.

Executive summary

3. The IRM Report 2020-21 considers the following:
 - are records being destroyed at the appropriate time
 - are records held for the appropriate time
 - is information held securely
 - is personal data being lawfully processed
 - are appropriate back-up arrangements in place
 - are key documents being managed in line with the C5 Key Documents Handbook
4. The IRM Report 2020-21 identifies a good level of compliance with our Information and Records Management Policy and the procedures set out in the Information and Records Management Handbook.
5. The IRM Report 2020-21 also identifies two areas where further work is required
 - (i) the development and implementation of revised retention and destruction processes in VC – this work will be undertaken in 2021-22 as part of the review of the Records Management Plan
 - (ii) a project to consider and recommend a way forward for the management of Key Documents and reviews – this work will be undertaken in 2021-22 as part of the review of the Records Management Plan

Assurance

6. Taking account of the IRM Report 2020-21, I am able to provide assurance that, as far as I am aware, the Commissioner's information and records are being managed in accordance with the Commissioner's policies and procedures and that:
- records are being destroyed at the appropriate time (as far as possible)
 - records are held for the appropriate time
 - information is held securely
 - personal data is being lawfully processed
 - appropriate back-up arrangements are in place
 - key documents are being managed in line with the Key Document Handbook.

COVID-19 pandemic

7. Temporary business continuity arrangements have been activated due to the impact of COVID-19 pandemic on the work of our office. As a result of these arrangements the office premises have been temporarily closed from 23 March 2020 and all members of staff are now working remotely with remote access to the office systems. Guidance on managing information has been provided to staff as part of the business continuity arrangements and details of this is set out in the attached assurance report.

Risk impact

8. This assurance report and our information management processes and procedures contribute to the control measures aimed at reducing the likelihood and impact of risk of the information we hold not being managed properly and held securely.

Equalities impact

9. No equality issues arise from this committee report.

Resources impact

10. The two actions to be carried referred to paragraph 5 above will require additional staff resource and it is anticipated that this can be met from existing staff resources.

Privacy impact

11. There are no privacy impact issues arising from this assurance report.

Operational/ strategic plan impact

12. None identified.

Records management impact (including any key documents actions)

13. None identified.

Consultation and Communication

14. QSMTM minute and the publication of this committee report.

Publication

15. I recommend that this CR is published in full but that paragraphs 12, 15, 32, 33 and 34 of the IRM Report 2020-21 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 a request were, at this stage, to be made for the information

Information and Records Management Report 2020-21

Provide assurance that the Commissioner's information and records are being managed in accordance with published policies and procedures, in particular that:

- records are being destroyed at the appropriate time
- records are held for the appropriate time
- information is held securely
- personal data is being lawfully processed
- appropriate back-up arrangements are in place
- key documents are being managed in line with the Handbook

Are records being held for the appropriate time?

File Plan and Retention Schedule (VC72711) (the Schedule)

1. The Schedule contains detailed rules for the retention of our records. The content reflects statutory and business requirements but is being updated as part of our work on UK GDPR implementation - the relevant retention periods relating to personal information are set out in our Privacy Notice which can be viewed here:

<http://www.itspublicknowledge.info/home/privacy.aspx>

2. The Schedule has been applied to the extent described above.

Simply Personnel (SP)

3. Following the closure of the office premises on 23 March 2020 due to the impact of COVID-19, it was not possible to access SP for recording annual leave and ill health leave between 1 April 2020 - 30 September 2020. Amended procedures were in place during this time to ensure that annual leave and ill health were recorded appropriately.
4. As all staff are working remotely and have access to our office systems, SP was updated and was able to be used again from 1 October 2020. SP operates in the same way as when the office premises were open - line managers approve (or not) requests to take annual leave and ill health leave is also recorded.
5. The SP system is a very basic system and information is held securely and access restrictions are in place. However, there is currently no process for the management of the content of the SP database and we are unable to delete the personal details held for former employees. We retain such data for 7 years following the termination of a contract of employment. As SP was implemented in 2014, in 2021-22, we will be procuring a different system which will enable us to manage the content of the database going forward.
6. Work on the retention plan for SP was delayed in 2020-21 due to the impact of the COVID-19 pandemic this and this work will now take place in 2021-22 and will be aligned with the work set out in above.

Are records being destroyed at the appropriate time?

7. There are procedures in place for the archiving/deletion of information held in Workpro and ACT! and, generally, these work well with information being archived and deleted in accordance with these procedures.
8. Processes for the management of Outlook, P and Z drives and paper records are also implemented routinely although it was not possible to remind staff to do so in Q1 as not all staff were able to work remotely. Guidance on records management has been issued to all staff who working remotely and have remote access to the office systems.
9. The project to revise the retention periods for records held in Virtual Cabinet (VC) was put on hold pending preparations for GDPR implementation. This project restarted in 2019-20 and will be now be carried forward into 2021-22 following the review of the Records management Plan. It is hoped that we will be able to create some automated processes and tasks to support the records review processes subject to our duties and responsibilities as regards data protection and personal information.
10. Once revised retention periods have been agreed, further work will be required to configure VC to perform any new automated processes in line with the agreed retention periods.

Is information held securely?

11. Various improvements arising from a security review which took place in 2015-16 were implemented and security was further reviewed as part of GDPR implementation in 2017-19.
12. [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
13. We received Cyber Essentials and Cyber Essentials Plus reaccreditation in December 2020 and March 2021 respectively.
14. We have in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed and these were followed in 2020-21.
15. [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]



- 16. When working remotely, all members of staff are still bound by our requirements regarding the security of information and have been advised to comply with the key document C5 Information and Records Management Handbook.
- 17. As far as I am aware, all members of staff have complied with the above as far as possible.
- 18. Access to personal information has also been limited to only those employees, agents, contractors and other third parties who are permitted to access this information.

Data incidents

- 19. We have in place procedures to manage and report any data incidents and notify and seek advice from the DPO when a data incident takes place. We have a data incident log and, also, have in place procedures for notifying the ICO of a data breach where we are legally required to do so. These procedures were followed in 2020-21.
- 20. In 2020-21 there were a total of 6 data incidents, only one of which was reported to the ICO. The other 5 incidents were minor and did not need to be reported to the ICO. The DPO has been consulted on all data incidents and the SMT has approved the recommended actions.
- 21. The table below provides a summary, for each quarter, of the number of data incidents and the action taken.

Data Incidents 2020-21			
	Number	DPO consulted	Reported to ICO
Q1	1	Yes	Yes
Q2	1	Yes	No
Q3	2	Yes	No
Q4	2	Yes	No
Total	6		

- 22. In 2021-22, we will also be looking at how to record near misses so that we can learn from these too.
- 23. Taking account of the above, I am satisfied that there were sufficient processes were in place in 2020-21 to ensure that information was being held securely.

Personal data is being lawfully processed

- 24. Most of the personal data we process is provided to us directly for one of the following reasons:
 - by an employee of the Commissioner or by someone who has applied to work with the Commissioner
 - by an enquirer making an enquiry to the Commissioner
 - by an applicant making an application (appeal) to the Commissioner

- by a representative of a Scottish public authority subject to FOI legislation
- by a person making an information request or subject access request to the Commissioner
- by a person indicating they wish to attend, or having attended, an event organised by the Commissioner
- by a person subscribing to our email and newsletter services
- by a complainant making a complaint to the Commissioner
- by a person making a whistleblowing complaint to the Commissioner
- by a person or company providing contracted services to the Commissioner

25. We may also receive personal information indirectly, in the following scenarios:

- we have contacted a Scottish public authority about an appeal made to the Commissioner and it provides personal information about another person as part of the investigation
- an applicant provides personal information about another person in their application correspondence
- an applicant provides personal information about another person in their correspondence when making an information request or subject access request to the Commissioner
- a complainant provides personal information about another person in their complaint
- a person making a whistleblowing complaint provides personal information about another person in their reporting to us
- we have received personal information about another person from other public authorities, regulators or law enforcement bodies
- an employee of the Commissioner provides personal information about another person, for example contact details, emergency contact details or a referee

26. The Commissioner's Privacy Notice, which is regularly reviewed and updated, provides comprehensive information regarding the personal data processing undertaken by the SIC and can be viewed here:

<http://www.itspublicknowledge.info/home/privacy.aspx>

Data protection at the end of the EU transition period

27. The UK left the EU on 31 January 2020 and the transition period ended on 31 December 2020. The Trade and Co-operation agreement concluded between the EU and the UK on 24 December 2020 sets out preferential arrangements in areas such as trade in goods and in services, digital trade, intellectual property, public procurement, aviation and road transport, energy, fisheries, social security coordination, law enforcement and judicial cooperation in criminal matters, thematic cooperation and participation in EU programmes. The agreement also includes some references to data protection.

28. As regards relevant terminology, we now operate under the "UK GDPR" with references to

the EU's version being the "EU GDPR". Our contracts, policies, procedures, correspondence and relevant documentation should now refer to "UK GDPR", where appropriate, to distinguish the difference between these regimes.

29. A positive adequacy decision is expected within the first half of 2021 and, in the meantime, a bridging mechanism is in place which:
- is intended to protect data flows during adequacy gap
 - will last for 4 months, with the possibility of a 2 month extension
 - will fall away when data adequacy is granted
30. The HOCS and the GDPR Working Party are keeping the above under review to ensure that any required organisational changes are put in place.
31. As far as I am aware, personal data is being lawfully processed in a way that is lawful and correct in accordance with the DPA 2018 and UK GDPR principles and, also, in accordance with our published policies and procedures.

Are appropriate back-up arrangements in place?

32. [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Are Key Documents being managed in line with the Handbook?

35. Key documents have been reviewed and there is a streamlined process for non-substantive planned reviews to assist progress.
36. To assist with reviews, the Review Schedule is considered every two months by the SMT. However, due to the temporary closure of the office premises and limited access to remote working systems, consideration of the Review Schedule was deferred in Q1 and commenced again in Q2.
37. A project to consider and recommend a way forward for the management of key documents and reviews is due to be undertaken in 2021-22.
38. I am satisfied that there are appropriate processes in place for the management of key documents and that, generally, key documents have been created and managed in line with

the C5 Key Documents Handbook. If any key document has been created or amended/approved out with the relevant procedures, the Responsible Manager should ensure that corrective action is taken within Q1 2021-22 to ensure that the key document has been amended and approved in line with the procedures set out in C5 Key Documents Handbook.

COVID-19 pandemic

39. The SMT activated temporary business continuity arrangements due to the impact of the COVID-19 pandemic on the work of our office and our office premises have been temporarily closed since 23 March 2020. As a result, not all members of staff were able to work remotely until the first part of Q2. All members of staff are now working remotely with remote access to our office systems.
40. Additional guidance on managing information securely has been provided to all members of staff working remotely.
41. All data protection and EU GDPR and UK GDPR requirements have continued to apply. For Q1 and the initial part of Q2 revised reporting arrangements for data incidents were in place.

