

**From: Stuart Gardner
Data Protection Officer
4 September 2018**

**Sarah Davidson,
Senior Information Risk Owner**

REVIEW OF DATA HANDLING COMPLIANCE – ALLEGED BREACH

1. Purpose

1.1 This report sets out the findings of the Data Protection Officer in reviewing compliance with the SG's data handling obligations regarding the alleged unauthorised disclosure of official information that appeared in the press between 24 and 26 of August 2018.

2. Action

2.1 The Senior Information Risk Officer is asked to note the findings in this document and the conclusion that no further action is required in light of the findings.

3. Background

3.1 Details of a complaint made by staff, in January 2018 under the Scottish Government procedure for handling harassment, appeared in the press on Friday 24 August and over the following weekend.

3.2 On Monday 27 August, The Scottish Government Senior Information Risk Officer asked the Data Protection Officer to review information handling procedures around the processing of these complaints within Scottish Government. The scope of the Review is set out at Annex A.

3.3 Allegations about a potential breach have been made directly to the Permanent Secretary. No communication regarding this allegation has been reported to the Scottish Government Data Protection Officer mailbox address given on the corporate website.

4. Review Method

4.1 Although we are only dealing with an allegation of an information breach the established process set out in the Information Asset Owners Handbook for investigating an actual data breach has been followed. In order to protect the integrity of the review, necessary adjustments to the roles were made to ensure a separation between the review and those staff who have had access to the documents in scope. Specifically, the Data Protection Officer replaced the Information Asset Owner as investigating officer. The review focussed on:

OFFICIAL SENSITIVE: DATA HANDLING COMPLIANCE

- 4.1.1 The handling and processing of relevant information within the Scottish Government for which the Permanent Secretary has responsibility;
- 4.1.2 Identifying and examining any evidence of unexplained transmission of relevant information to internal or external parties between February 1 February and 24 August 2018;
- 4.1.3 The arrangements for the release by the SG of relevant information to the Crown Office and Procurator Fiscal Service (COPFS) and Police Scotland.

4.2 The review obtained IT system logs relating to the use of the Scottish Government's email and electronic record management system by individual members of staff known to have had access to relevant documents (listed at Annex B). Interviews were held with staff to establish if correct procedures have been complied with.

5. Findings

5.1 Information Handling

5.1.1 Relevant records of processing and the legal basis for HR related material in eRDM and SCOTS e-mail are recorded in the Information Asset Register and Information Asset Owners are defined.

5.1.2 All 23 staff identified as having access to the relevant material (except one on long-term absence) have successfully completed GDPR specific information handling training this year.

5.1.3 Access to relevant material was controlled electronically by SCOTS account and application specific access management. Paper formats have been controlled through the use of locked cupboards and safes. Electronic transfer of information made use of secure networks.

5.1.4 Staff interviewed were aware of information handling responsibilities and no evidence of deliberate or accidental unauthorised disclosure was identified.

5.1.5 I am therefore able to conclude that the staff within scope of this review have complied with all of the relevant information handling procedures and obligations (with the exception of the GDPR training by the staff member on long-term sick leave, who anyway had limited access to the relevant information).

5.2 Cyber Security

5.2.1 Electronic Records Management System logs were examined by iTECS system managers who looked at access by the authorised staff listed at annex B, and also by the information management support officers (IMSO) for the business areas, who have not been involved in any part of the harassment investigation but who have system administration privileges. There was no

evidence of any unauthorised access to the documents held in this area and no access at all by IMSO staff.

5.2.2 A scan of the SCOTS storage system for the relevant documents was undertaken by iTECS cyber security staff. Only files held by authorised staff who were part of this review were identified. No unauthorised staff are holding copies of relevant material on their work accounts.

5.2.3 Outbound e-mails logs for relevant staff were examined by iTECS cyber security team covering the period from 28 January 2018. This examined all email activity regardless of subject matter. There was no evidence of any emails going to media outlets from those members of staff. iTECS also examined any email traffic from any SCOTS users to media outlets since 1st June (this being as far back as online records allow). There is no evidence that any SCOTS user sent anything related to the harassment investigation to any media outlet in the period since 1 June 2018.

5.2.4 From the above technical searches of the SG's corporate systems I am able to conclude with reasonable confidence that there is no evidence of any communication between media outlets and relevant staff through the SCOTS system. The searches also indicate that no other member of staff sought to gain unauthorised access to relevant information held on SG systems nor used the SCOTS systems to communicate relevant information to any unauthorised person, internally or externally.

5.3 Data Sharing

5.3.1 Documents relating to this review have been managed within the secure SCOTS environment and processed by People Directorate under a GDPR compliant legal basis recorded in the information asset register. Transfers to a range of other stakeholders were necessary:

- **Original Complainants** were provided with copies of relevant material to their personal e-mail accounts from the SCOTS network. This was done under People Directorate's legal basis for processing – legitimate interest.
- **Queen's Counsel** was provided with copies of relevant material by e-mail from the SCOTS network to the secure CJSM network. This is a declared record of processing on the information asset register under legal obligation.
- **The First Minister's Principal Private Secretary** (John Somers) was provided with a summary document providing an overview of the investigation process, but not including in whole or in part the source investigatory documents. This summary document was e-mailed within the SCOTS network. The summary document was shared in hard copy with the First Minister using appropriate information handling protocols. This is a declared record of processing on the information asset register under public task.
- **The Former First Minister, and subsequently solicitors working on his behalf**, were provided with copies of relevant material by e-mail from the SCOTS network.

- **Crown Office and Procurator Fiscal Service** was provided with copies of relevant material by hand by a named civil servant who was authorised to view the material and has been part of this review.

5.3.2 No Information relating to this review was provided by Scottish Government to Police Scotland.

6. Conclusions

6.1 The review into data handling compliance showed that information relating to the original investigation was processed in a controlled and compliant manner.

6.2 The forensic searches of our corporate systems have not detected any evidence of a data breach.

6.3 In light of these conclusion, I am not proposing to take any further action in terms of the alleged breach.

Stuart Gardner

Data Protection Officer
Scottish Government

4 September 2018

Annex A – Scope of review agreed with Senior Information Risk Officer

Annex B – List of staff with access to relevant material

Annex A – Scope of review agreed with Senior Information Risk Officer

REVIEW OF DATA HANDLING COMPLIANCE – ALLEGED BREACH

1. Purpose

1.1 This note sets out the steps that will be taken by the Data Protection Officer (DPO) to review compliance with the SG's data handling obligations regarding the alleged unauthorised disclosure of official information that appeared in the press between 24 and 26 of August 2018.

2. Timing

2.1 The DPO will aim to complete the review as a matter of the highest priority.

3. Scope

3.1 The review will follow the established process set out in the Information Asset Owners Handbook. In order to protect the integrity of the review, any necessary adjustment to the roles set out in the established process will be made to ensure a separation between the review and those staff who have had access to the documents in scope of the review. Any required adjustments to roles will be recorded in the final report.

3.2 The review will focus on:

- 3.2.1 The handling and processing of relevant information within the Scottish Government for which the Permanent Secretary has responsibility;
- 3.2.2 Identifying and examining any evidence of unexplained transmission of relevant information to internal or external parties;
- 3.2.3 The arrangements for the release by the SG of relevant information to the Crown Office and Procurator Fiscal Service (COPFS) and Police Scotland. (Both organisations will be advised that the SG is undertaking this review.)

3.3 The review will include obtaining systems logs relating to the use of the Scottish Government's email and electronic record management system by individual members of staff known to have had access to relevant documents. Contact will be made with those staff to establish if correct procedures have been complied with.

Out of Scope

3.4 The review will not:

- 3.4.1 Engage with any individual who raised a complaint or was the subject of a complaint under the Harassment procedure;
- 3.4.2 Review the data handling arrangements within the Crown Office and Procurator Fiscal Service (COPFS) or Police Scotland.

4. Reporting

4.1 A report setting out the outcomes of the review will be prepared by the DPO and submitted to the Senior Risk Information Owner.

Stuart Garnder
Data Protection Officer
Scottish Government

29 August 2018

OFFICIAL SENSITIVE: DATA HANDLING COMPLIANCE

Annex B – List of staff with access to relevant material

Staff Member	Interviewed
Paul Cackette	Yes
Caroline Beattie	Yes
[REDACTED]	Yes
Barbara Allison	Yes
[REDACTED]	Yes
Leslie Evans	Yes
Sarah Davidson	Yes
Colin Troup	Yes
[REDACTED]	Yes
John Somers	Yes
Nicky Richards	Yes
[REDACTED]	Yes
[REDACTED]	Yes
[REDACTED]	Yes
Judith Mackinnon	Yes
[REDACTED]	Yes
Liz Lloyd	Yes