

**NORTHWEST TERRITORIES  
INFORMATION AND PRIVACY COMMISSIONER**

Review Report 20-238

Citation: 2020 NTIPC 39

File: 19-234-4

July 27, 2020

## **BACKGROUND**

On September 17<sup>th</sup>, 2019, our office received a privacy breach complaint from an employee with the Department of Education, Culture and Employment (ECE). The concern was about the apparent mismanagement of his performance appraisal records. He advised that he had a first performance appraisal meeting with his supervisor and was then told he was to have his response and comments entered formally to “the system” by a particular date, which deadline was subsequently extended several times. Between the date of the meeting and the day that the response was due, the Complainant’s supervisor apparently added new comments to the written version of the appraisal document. The Complainant requested additional time to respond. At some point later he received a notice that his performance document had been closed and could not be accessed. A new document was eventually opened for the Complainant’s use.

The day before the new deadline, the Complainant tried to complete the performance appraisal document in the electronic system but his comments were not appearing in the appropriate field of the competencies section of the document, apparently because his supervisor had closed the system to him earlier than the stated deadline, locking him out of the system. After a request, the system was re-opened to him and he completed the document as required. Several days later, he received a notice that the performance document had again been closed.

Several months later, when the matter again came to the fore, the job performance document could not be located in the HRIS SAM system and the Complainant was asked to complete the document for a third time.

The Complainant was suspicious of the ongoing problems with his performance appraisal. He and his supervisor appear to have had some differences of opinion and the Complainant alleged that the problems with the completion of the performance appraisal form was being orchestrated by his supervisor.

He considered all of this a mismanagement of his personal information resulting in unauthorized collection, use or disclosure under the ATIPP Act.

### **THE DEPARTMENT'S RESPONSE**

The Department advised that the GNWT performance management system is an electronic process. Performance documents are completed electronically via the GNWT's Human Resource Information System (HRIS). They note that the HRIS is

a secure site, password encrypted, with safety measures in place to ensure information entered into the Performance Document can only be seen by the employee, their supervisor, the Review Officer (supervisor's supervisor) and the Performance Development Administrators.

The Department provided a detailed, step by step, explanation in relation to the Complainant's performance evaluation. There were clearly some glitches along the way. At one point there were, apparently, duplicate versions of performance appraisals of several of the employees in the Complainant's division and the Supervisor asked the Performance Development Administrators to remove the blank copies. This resulted in the cancellation of the wrong version of the Complainant's Performance Document – instead of cancelling the blank version, the partially completed version was mistakenly cancelled. This version was eventually restored so that the Complainant could complete his part of the document. There were some additional technical problems in that it

appears that some of the information the Complainant was trying to add was not visible when saved.

It also appears fairly clear that there were communication issues between the Complainant and his supervisor that did not help the situation. In the end, however, no records were ever “lost”. Two documents for the Complainant were “cancelled”. Both were completely blank. This does not mean that they were deleted or otherwise lost. Rather both were still accessible in a tab in the HRIS called “Historical Documents”. Documents in this tab or folder cannot be altered by anyone, including the employee. The third document contained all of the necessary information, both from the supervisor and from the Complainant.

## **DISCUSSION AND CONCLUSIONS**

The *Access to Information and Protection of Privacy Act* dictates how and when and for what purposes public bodies can collect, use and disclose personal information.

The information in a performance review record is, without a doubt, personal information. The Act requires that personal information in the custody and control of a public body must be protected from unauthorized collection, use and disclosure. In particular, Section 42 provides:

42. The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Section 43 sets out those circumstances in which personal information can be used by a public body as follows:

43. A public body may use personal information only
- (a) for the purpose for which the information was collected or compiled, or for a use consistent with that purpose;
  - (b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use; or
  - (c) for a purpose for which the information may be disclosed to that public body under Division C of this Part.

In this case, there is no allegation or indication that the Complainant's personal information collected for the purpose of completing a performance review was used for any purpose but the performance appraisal - which is a function of the management of personnel and is a legitimate and authorized purpose for the collection and use of personal information.

This leaves the question of whether or not there was an unauthorized disclosure of the Complainant's information in the confusion of the process of completing the documents.

While there were clearly problems with how the system worked, there is no indication that the information in question ever left the confines of the HRIS system or that any unauthorized person ever had access to the records. The Complainant's information may have been shunted around within the system, but there is no indication that it ever left the system.

It appears that all versions of the document in question were at all times protected by appropriate access safeguards while in the system. Nor is there any indication or suggestion that the Complainant's personal information was inappropriately viewed while in the HRIS system.

While there may be some technical issues that need to be fixed in terms of how information is inputted and saved, there is nothing in the circumstances described to me that suggests that there was any unauthorized collection, use or disclosure of the Complainant's personal information. The system itself had the security functions necessary to restrict access to the records in the system - whether they were in the "Historical Documents" folder or in the part of the system which allowed the Complainant to enter his comments.

I therefore find that there is nothing to suggest that there was an inappropriate collection, use or disclosure of the Complainant's personal information and I make no recommendations.

Elaine Keenan Bengts  
**Information and Privacy Commissioner**