OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report A-2024-047

October 18, 2024

Memorial University

Summary: Memorial University received an access request for certain email records sent by a senior University official. The University responded that the official had used his personal email account, not a University email account, and that a search had failed to locate any responsive records. The Complainant filed a complaint with our Office. The Commissioner concluded that the University had conducted a reasonable search for records, that the explanation for failing to locate any records was reasonable, and that there was insufficient evidence to conclude an offence had been committed. The Commissioner, however, recommended that the University create a clear and enforceable policy requiring all employees and officials to use a Memorial University email account, not a personal email account, for University business.

Statutes Cited: Access to Information and Protection of Privacy Act, 2015, SNL 2015, c. A-1.2, sections 13, 115.

Management of Information Act, SNL 2005 c. M-1.01.

Authorities Relied On: NL OIPC Report A-2016-021;

OIPC Guidance on Use of Personal Email Accounts for Public Body Business;

Office of the Chief Information Officer Directive on Non-Governmental Email Accounts.

BACKGROUND

[1] The Complainant made an access request under the **Access to Information and Protection of Privacy Act, 2015** (ATIPPA, 2015) to Memorial University on June 28, 2024. The request sought emails from a named official, (the Chair of the University's Board of Regents), on a specific topic, between the dates of June 19, 2024 and June 27, 2024.

[2] The University's response to the request was that a search had been conducted, but no records responsive to the request were located. The Complainant filed a complaint with our Office.

[3] As informal resolution was unsuccessful, the complaint proceeded to formal investigation in accordance with section 44(4) of ATIPPA, 2015.

ISSUES

[4] There are three issues to be dealt with in this Report :

1. Whether Memorial conducted a reasonable search for responsive records;
2. Whether Memorial provided a reasonable explanation for the failure to locate records; and
3. Whether there is evidence of an offence under ATIPPA, 2015.

DECISION

[5] Section 13 of ATIPPA, 2015 provides:

> 13.(1) The head of a public body shall make every reasonable effort to assist an applicant in making a request and to respond without delay to an applicant in an open, accurate and complete manner.

[6] This includes the duty to conduct a reasonable search to locate and identify responsive records. What constitutes a reasonable search may vary with the circumstances, but generally must be conducted by knowledgeable staff, in locations where the records in question might reasonably be found.

[7] In the present case, staff from the University's Information Access and Privacy Office asked the named official to search his email records. The official did not use the @mun.ca email address that had been provided to him for MUN business, but consistently used his personal email address. The email address used was in fact the email account for the official's personal business. This Report, in reflecting our guidance documents on this topic, will refer to any non-public body email account as a "personal" email. The University was unable to directly search the official's personal email, and so it requested that the official conduct the search himself, using search terms provided.

[8] However, the official had previously reported to other officials at Memorial that he was experiencing technical difficulties with his personal email account, and had recently had to delete many of his messages. After being advised of the access request, the official reported that although he conducted the search as requested, no responsive records were located.

[9] In their submissions, the Complainant raised the issue of whether the official may have deleted the messages after being informed of the access request. However, the evidence before us suggests the official had actually deleted the messages, and notified others of the problem, asking them to re-send some messages, prior to his being notified of the access request.

[10] The Complainant advises that they made a further access request in September for records related to the above search. This request revealed the request to the official to search his records was mainly conducted by telephone, rather than by MUN's usual written process and forms. The Complainant submits that the lack of a well-documented search ". . . erodes any confidence in transparency."

[11] ATIPPA, 2015 does not dictate how a public body should conduct a search for records or how it should document how it has handled an access request. However, having a written record of how a request was processed, and documenting efforts to locate records, is a best practice. In this particular case, there are factors present which would demand that the search be carefully documented: this was a request for records from a very senior official, this senior

official was facing accusations of wrongdoing in his email correspondence, the records were not in the possession of the University, and the search relied entirely on that official to search his own personal email account for potentially embarrassing records.

[12] It should be noted that the official concerned is no longer a member of the University administration. The University indicated that it is therefore no longer able to obtain further information or cooperation from the individual, or to request a further search.

[13] Despite the shortcomings in the University's documentation of its search, the evidence suggests that there was a technical issue with the official's personal email which developed in the weeks prior to June 19, 2024 and June 27, 2024 and any responsive emails were deleted prior to the official being made aware of the request on July 2, 2024. As such, by the time the access request had been made, there were no apparent records that the University could have located with its search.

[14] In their complaint and subsequent submissions, the Complainant asked our Office to investigate whether an offence may have been committed. Section 115 of the Act makes it an offence for anyone to willfully mislead or obstruct the Commissioner or another person performing duties under the Act, or to destroy a record subject to the Act with the intent to evade an access request. However, the information currently available to this Office is not sufficiently conclusive to support laying charges under section 115 of ATIPPA, 2015.

[15] The Complainant also queried whether the actions of the University official would constitute a breach of the University's Code of Conduct. That is something over which we have no jurisdiction, and so we cannot comment on that issue. This would be an issue that the Complainant may wish to pursue in a separate process.

[16] We can, however, comment on the use by a University official of their personal email for University business. This issue is core to the questions and complaints raised in this investigation. Our Office takes the view that every public body should have, and should enforce, a clear policy prohibiting such practices. See, for example, our guidance on Use of Personal Email Accounts for Public Body Business and our Report A-2016-021.

[17] It is clear to us, and the University agrees, that regardless of the method used to communicate, such messages are subject to ATIPPA, 2015 and to Memorial's privacy and information management policies. However, while Memorial has apparently provided its employees and officials with @mun.ca email accounts, there is at present no policy requiring officials to actually use them.

[18] From the information provided to us, it appears that Memorial was in fact aware that officials were using their personal email accounts rather than the @mun.ca accounts provided to them, and regularly communicated with several officials using their personal email accounts. Memorial should have recognized that this was inappropriate and taken steps to develop a policy to eliminate this practice. The Complainant submits that "this is, at a minimum, a serious procedural issue which invites all sorts of privacy and information management issues and, at worst, a deliberate attempt to obfuscate accountability and transparency."

[19] We note that the provincial government's Office of the Chief Information Officer has issued a Directive with respect to the use of non-government email for work purposes. This directive makes it clear that, subject to clearly approved and documented exceptions in limited cases, the use of personal or non-government email accounts to conduct work on behalf of a public body is not permitted.

[20] The Directive was created under the legislative authority of the **Management of Information Act**. As the Directive itself states, the Management of Information Act:

> . . . requires departments and other public bodies to manage and protect government records regardless of format; this includes email. Government records exist to document and support the activities of the department or other public body and to support transparency and accountability of the Government of Newfoundland and Labrador.
>
> Individuals provided with a government-issued email account are expected to use it for business purposes. Use of a non-government email account to conduct work on behalf of a department or other public body is not permitted.
>
> This Directive applies to all government departments and other public bodies as defined under the MOIA and issued under the authority of the Information Management and Protection Policy (IM&P) Policy. The IM&P Policy establishes

> the foundation for development of all IM&P policies, directives, standards, guidelines and procedures by the OCIO and provides the OCIO with a comprehensive approach in addressing IM&P Policy governance.

[21] Memorial University is a public body as defined by section 2(d)(iii) of the Management of Information Act.

[22] If a public body does not create, and enforce, a policy requiring all of its members to use official email accounts for public body business, problems can arise, both for effective information management and for compliance with ATIPPA, 2015, as the present case illustrates. In the days just prior to the issuing of this Report, Memorial has advised that the new Chair of the Board of Regents has issued a directive to all board members requiring they use their @mun.ca email addresses for board business. This is a welcome development; However, the issue warrants a University-wide, enforceable policy which covers all members of the University community., rather than a personal directive by the new Chair of the Board of Regents,

RECOMMENDATIONS

[23] Under the authority of section 47 of the **Access to Information and Protection of Privacy Act, 2015** (ATIPPA, 2015), I recommend that Memorial University create a clear and enforceable policy within three months which requires all employees and officials to use the University's internal email account, not a personal email account, for University business.

[24] As set out in section 49(1)(b) of ATIPPA, 2015, the head of Memorial University must give written notice of his or her decision with respect to these recommendations to the Commissioner and any person who was sent a copy of this Report within 10 business days of receiving this Report.

[25] Dated at St. John's, in the Province of Newfoundland and Labrador, this 18th day of October 2024.

Jacqueline Lake Kavanagh
Information and Privacy Commissioner (Acting)
Newfoundland and Labrador