ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2021-33

September 1, 2021

EDMONTON CATHOLIC SEPARATE SCHOOL DIVISION

Case File Number 005967

Office URL: www.oipc.ab.ca

Summary: The Applicant, a former employee, made an access request under the *Freedom of Information and Protection of Privacy Act* (the FOIP Act) to the Edmonton Catholic Separate School Division (the Public Body) for records in particular departments containing his name.

The Public Body conducted a search for responsive records. It provided the responsive records it located to the Applicant, but severed some information from them under sections 17(1) (disclosure harmful to personal privacy) and 24(1) (advice from officials) of the FOIP Act.

The Applicant requested review by the Commissioner of the adequacy of the Public Body's search for records and its decisions to sever information from them.

The Adjudicator confirmed that the Public Body conducted a reasonable search for responsive records. The Adjudicator also confirmed the Public Body's decision to sever information under section 24(1). The Adjudicator confirmed the decision of the Public Body to sever information regarding employee absences, but directed it to disclose the remainder of the information to which it had applied section 17(1) to the Applicant.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c F-25, ss. 1. 10, 17, 18, 24, 25, 72

Authorities Cited: AB: Orders F2003-005, F2004-026, F2007-012, F2007-029, F2013-51, F2015-29, F2019-09, F2021-28

Cases Cited: *Edmonton (City) v Alberta (Information and Privacy Commissioner)*, 2016 ABCA 110 (CanLII)

1. BACKGROUND

[para 1] The Applicant, a former employee, made an access request to the Edmonton Catholic Separate School Division (the Public Body) for the following records:

> **Human Resources Department**
> - A copy of my personnel file
> - Any emails or Skype for business communication, where my name is mentioned
> - Any meeting minutes where my name or the name of the Finance Security project is mentioned
> - Any investigations where my name is mentioned
>
> **IITS Department**
> - Any meeting minutes or results, where my name or the name of the Finance Security project is mentioned
> - Any investigations, where my name or the name of the project I was working on is mentioned
>
> From the following individuals that work in IITS Department:
> - […]
>
> 1. I request to see all incoming and outgoing emails and all incoming and outgoing Skype for Business messages where my name or the name of the Finance Security Project is mentioned.
>
> 2. I request any files or actual printed documents, where my name or the name of the project I was working on is mentioned
>
> **Finance Department**
> - Any meeting minutes or results, where my name or the name of the Finance Security project is mentioned
>
> - Any investigations, where my name or the name of the project I was working on is mentioned
>
> From the following individuals that work in the Finance Department (the last names of some individuals working in Finance is missing or misspelled, however, their first name is the only such first name in the department):
>
> [,,,]
>
> l. I request to see all incoming and outgoing emails and all incoming and outgoing

> Skype for Business messages, where my name or the name of the Finance Security Project is mentioned.
>
> 2. I request any files or actual printed documents, where my name or the name of the project I was working on is mentioned.

[para 2] The Applicant asked the Commissioner to review the Public Body's response to his access request. In particular, he questioned the adequacy of the Public Body's search methods for responsive records and its decisions to sever information from the records it located.

II. ISSUES

ISSUE A: Did the Public Body meet its duty to the Applicant as provided by section 10(1) of the Act (duty to assist applicants)?

ISSUE B: Does section 17(1) of the Act (disclosure an unreasonable invasion of personal privacy) apply to the information to which the Public Body applied this provision?

ISSUE C: Did the Public Body properly apply section 24(1) of the Act (advice from officials) to the information in the records?

III. DISCUSSION OF ISSUES

ISSUE A: Did the Public Body meet its duty to the Applicant as provided by section 10(1) of the Act (duty to assist applicants)?

[para 3] Section 10(1) of the Act states:

> *10(1) The head of a public body must make every reasonable effort to assist applicants and to respond to each applicant openly, accurately and completely.*

[para 4] In Order F2007-029, the Commissioner made the following statements about a public body's duty to assist under section 10(1):

> The Public Body has the onus to establish that it has made every reasonable effort to assist the Applicant, as it is in the best position to explain the steps it has taken to assist the applicant within the meaning of section 10(1).
>
> . . .
>
> Previous orders of my office have established that the duty to assist includes the duty to conduct an adequate search for records. In Order 2001-016, I said:

> In Order 97-003, the Commissioner said that a public body must provide sufficient evidence that it has made a reasonable effort to identify and locate records responsive to the request to discharge its obligation under section 9(1) (now 10(1)) of the Act. In Order 97-006, the Commissioner said that the public body has the burden of proving that it has fulfilled its duty under section 9(1) (now 10(1)).
>
> Previous orders . . . say that the public body must show that it conducted an adequate search to fulfill its obligation under section 9(1) of the Act. An adequate search has two components: (1) every reasonable effort must be made to search for the actual record requested and (2) the applicant must be informed in a timely fashion what has been done.

…

In general, evidence as to the adequacy of search should cover the following points:

- The specific steps taken by the Public Body to identify and locate records responsive to the Applicant's access request

- The scope of the search conducted – for example: physical sites, program areas, specific databases, off-site storage areas, etc.

- The steps taken to identify and locate all possible repositories of records relevant to the access request: keyword searches, records retention and disposition schedules, etc.

- Who did the search

- Why the Public Body believes no more responsive records exist than what has been found or produced

[para 5] The Public Body provided the following explanation of the search it conducted:

> Edmonton Catholic Schools follows a consistent process in performing searches for FOIP requests. In this specific case, based on the information provided by the FOIP Coordinator who led the search in 2017, an email with the wording of the request was sent to the heads of the three departments that were specifically identified in the Applicant's request. These heads were responsible for overseeing the searches conducted by their respective departments. Staff members in possession of responsive records were instructed to provide these records to their department heads. These are the records that the FOIP Coordinator processed and included in the release. This practice is consistent with the FOIP Act Guidelines and Practices Manual (Locating, Retrieving and Copying Records) along with the practices of other large public bodies, including the Government of Alberta.
>
> The areas searched by the three departments consist of the following:
>
> - IITS searched personal and shared drives/folders, as well as Outlook and the Skype for Business platform of named staff members.
> - HR provided the contents of the Applicant's electronic employee file (stored in SharePoint and uploaded via KnowledgeLakeConnect) and searched email

correspondence and the Skype for Business platform for those who worked on the Applicant's file.
- Finance searched Outlook, Office 365 folders, shared drives, and collaborative or shared sites located on myecsd.net. The Department advised that Skype for Business communications in Finance were not set up to be retained during the time of the request.

Staff members are instructed to provide all responsive records and to confirm that they have completed their search in accordance with the parameters of the request. Ultimately, the FOIP Coordinator oversees the search, and if necessary, requests that staff members expand their search if there is reason to believe that additional records may be located. Based on the volume and content of records returned during the initial search for records and because the Applicant was very clear in naming the timeframe, areas, repositories, and individuals to be included in the search, there was no reason to believe that an expanded search was necessary.

The Applicant raises four items which are based on two general concerns. The first concern that the applicant raises appears to suggest is that the individuals who are involved in the search are not impartial or neutral. The second concern that the applicant raises appears to suggest is that there may be missing records, specifically Skype for Business communications.

With regard to the first issue of impartiality, the duty to assist provisions of the *FOIP Act* do not require ECSD to have a "neutral party" conduct the search for records, as described by the Applicant. According to *Harelkin v. University of Regina [1979] 2 S.C.R. 561 (Orders F2007-0l2 [18], F2018-72 [43]):*

"However, where an applicant's primary argument was that the head of the public body was in a confllct-of-interest situation when he processed the applicant's access request, an Adjudicator did not agree with the applicant's argument that a conflict-of-interest results in a failure to meet the public body's duty to assist. Under the Act the head of the public body is accountable for any failures or omissions of the public body in responding to an access request. The head of *a public body, by the very nature of the position, will often hove duties* to *the public body that may compete with the head's duties under the Act."*

With regard to the second issue of the possibility of missing records, specifically Skype for Business communications, ECSD maintains that it made every reasonable effort to locate responsive records. Based on the information provided by the FOIP Coordinator who performed the search in 2017, the FOIP Coordinator sent an email with the relevant portions of the original request to senior staff members in the three departments named by the applicant - HR, IITS, and Finance. Each affected department was tasked with locating responsive records and consulted with the appropriate staff members to do so. Those involved in the records search used the wording of the request in determining the scope of their search. As seen in the original request, the Applicant was very specific in terms of the types of records requested, as well as the staff members that were to be included in the search. Following the conclusion of their respective searches, staff from the three departments confirmed via email that they had searched for and provided all records in accordance with the Applicant's request.

At the time of the search, ECSD consulted its staff members about the usage of the Skype for Business platform. The records relating to the platform are transitory in nature and are therefore disposed of once no longer necessary.

Additionally, the Applicant asserts that there were Skype for Business communications that were included in the release, therefore contradicting ECSD's position that records from that platform were transitory in nature. The "number of Skype for business communications" to which the

applicant refers to are only contained in a single email on pages 439 and 440 of the release package. This Skype for Business conversation was embedded within an email chain, which is why a record exists. ECSD would like to reiterate its position that in the process of locating records, no responsive Skype for Business records were found.

[para 6] The Applicant stated in his rebuttal submissions:

In their response they claim that they did everything possible to find all requested records, however, I strongly disagree. They claim that they have contacted the heads of relevant departments and those heads in turn contacted the employees involved. All those employees (including heads of departments, managers, supervisors, etc) were instructed to complete a search of their own records with the specific search terms and provide the results. This approach is not impartial, prone to mistakes and extremely flawed.

Below is a list of issues with this approach:

1. Each of these employees (including heads of departments, managers, etc) are not neutral parties (i.e. potentially have a conflict of interest) and might not willingly (in good faith) release all the relevant records that they have.
2. They might have deleted some of the relevant records and thus no longer have access to them. These deleted records are still on the ECSD server (because of a document retention policy) but the employees have no access to them.
3. Not all of these employees are technically competent to perform a records search of their own computer, their emails and their Skype for Business messages
4. In the attached email it is shown that many people were contacted to provide records. The more employees are involved the higher is a chance for errors.

It is a responsibility of the ECSD (public body) to prove that the record search that they have performed is adequate, accurate and complete. Their argument and the large chains of emails performed by different departments show that this wasn't so.

They could have done a professional records search. They do have a central email server where all the emails are stored (I believe Skype for Business messages are stored there as well). Their retention policy applies to all the information stored on that server. They should have instructed a technically competent professional (an individual who doesn't have a conflict of interest) or a group of professionals to perform a records search on that server. That type of search would avoid all of the issues mentioned above (i.e. deleted messages, neutrality, technical competency, etc). Also, it is important to note that the email server is per public body and not per department (departments do not have or maintain their own email servers).

Thus, I have the following three questions to ECSD:
1. Why wasn't a central email server search done?
2. Can they guarantee that the involved employees didn't delete any of their email messages?
3. Can they guarantee that each employee released all relevant information?
4. What is their records retention policy?

My response to them bringing up a 42 year old case of Harelkin v. University of Regina case is as follows:

> The case made a ruling with respect to a neutrality of a single employee (i.e. the head of the public body). In our situation there are many employees (around 10) that were requested to

> provide information. Each of them has a potential conflict of interest thus my concern is very valid. Also, in 1979 there weren't any computers. In the current case ECSD had a much better alternate way to perform a records search. They could have easily performed a much better search of requested records by pulling info from the central email server. This type of search would have been quicker, easier and more cost effective. I am disappointed to see how inefficiently ECSD uses taxpayer dollars in this situation.

[para 7] In its reply submissions, the Public Body provided further detail regarding the steps it took to locate responsive records which I will not reproduce here. It also explained why it believed no further records exist than have been produced:

> Throughout the process of locating records, the submitted records were reviewed/evaluated by the FOIP Coordinator at the time for completeness for all three identified departments. The FOIP Coordinator followed up with staff by requesting any missing attachments and/or records from the department staff as necessary. The FOIP Coordinator also sought for better versions of the records that may have not been legible. In reviewing the records, the FOIP Coordinator did not simply receive the records and proceed to process them, but also reviewed the records for completeness. In order to ensure that the request parameters were followed, the FOIP Coordinator requested all potentially responsive records from the staff even if the records would be considered non-responsive or confidential. Having the FOIP Coordinator review the file for completeness and determining responsiveness or confidentiality of the records was important in ensuring ECSD responded in an open, accurate and complete manner.
>
> […]
>
> Through the evidence provided, ECSD has demonstrated that it has made every reasonable effort to assist the Applicant openly, accurately and completely. The Applicant has failed to provide any concrete proof that ECSD has not performed its duty to assist the Applicant under section 10(1) of the Act. The Applicant has had multiple opportunities to provide proof (upon the receipt of the April 26th, 2017 submission, the OIPC Review process, the OIPC Inquiry submission and the OIPC Inquiry rebuttal), but has only objected to the impartiality and the competence of the ECSD staff to search for records. Both of these objections have been discussed and refuted by ECSD within this submission, therefore ECSD maintains that it has performed its duty to assist the Applicant under section 10(1) of the Act.
>
> The Applicant has not been able to identify any specific gaps within the records except for the supposed Skype for Business records that were included in pages 439-440 of the release. ECSD would like to reiterate that the reason these were included is because they were embedded in an email chain.

[para 8] The Public Body has provided detailed explanations of the search it conducted. I agree with the Public Body that its approach to the search was reasonable. Asking employees who are named in access requests, or who work in areas likely to have responsive records, to search for responsive records on their computers is a sensible method of beginning a search for responsive records.

[para 9] The Applicant argues that the Public Body should have conducted a central search of its computer systems, rather than having employees search their emails

and records. In Order F2007-012 I rejected an argument that a public body's response was flawed, simply because of the possibility of bias or conflict of interest. I said:

> I do not agree with the Applicant's argument that a conflict of interest results in a failure to meet the Public Body's duty to assist. Under the Act, the head of the public body is accountable for any failures or omissions of the public body in responding to an access request. The head of a public body, by the very nature of the position, will often have duties to the public body that may compete with the head's duties under the Act. Delegating the head's responsibility to respond to an access request to an employee such as a FOIP coordinator does not mitigate the potential for conflict of interest. For this reason, the Act provides individuals who have made access requests the right to an independent review of the head's decisions by a neutral third party, the Information and Privacy Commissioner. The independent review rectifies any issues of conflict of interest or potential bias. As the Applicant in this case has exercised his right to request an independent review, any miscarriage of natural justice he perceives will be remedied by the review. See *Harelkin* (*supra*).

[para 10] In the foregoing passage, I rejected the argument that bias alone was sufficient to call into question the adequacy of a public body's search for responsive records. I noted that the FOIP Act creates a right of independent review by the Commissioner to cure any defects in a search. In an inquiry by the Commissioner, a public body must establish the adequacy of its search through the introduction of evidence meeting the requirements of Order F2007-029. An applicant may test the public body's evidence, including by pointing to records that the applicant has reason to believe exist, but have not been produced. In this way, public bodies are held to account in relation to the searches they conduct under the FOIP Act.

[para 11] The Public Body has responded to the Applicant's specific concerns regarding Skype records and provided a detailed account of the search it conducted. It also provided detailed evidence as to how employees searched for responsive records.

[para 12] The Applicant has not pointed to records he believes to be missing from the search, or provided evidence regarding records he believes should exist, but were not produced. Instead, he argues that the search should have been conducted centrally, and he asserts, without foundation, that those employees who participated in the search for responsive records, lacked the skills to do so and may have deleted records.

[para 13] I find that the Public Body conducted a reasonable search for responsive records. It was open to the Public Body to search for responsive records using the process it did, and it has not been demonstrated in this inquiry that the central search proposed by the Applicant would have located any additional records beyond those the Public Body located. There is simply no evidence before me that the employees who searched for responsive records lacked competence, conducted inadequate searches, or deleted records.

[para 14] I confirm that the Public Body met its duty to assist the Applicant by conducting a reasonable search for responsive records.

ISSUE B: Does section 17(1) of the Act (disclosure an unreasonable invasion of personal privacy) apply to the information to which the Public Body applied this provision?

[para 15] The Public Body has applied section 17 to withhold information about employees' vacations, job titles, employment responsibilities and office room numbers and direct lines assigned to employees from the Applicant.

[para 16] Section 17 requires a public body to withhold the personal information of an identifiable individual when it would be an unreasonable invasion of the individual's personal privacy to disclose his or her personal information. Section 17 states, in part:

> *17(1) The head of a public body must refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.*
>
> *(2) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if*
>
> […]
>
> *(e) the information is about the third party's classification, salary range, discretionary benefits or employment responsibilities as an officer, employee or member of a public body or as a member of the staff of a member of the Executive Council* […]
>
> […]
>
> […]
>
> *(4) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if*
>
> […]
>
> *(d) the personal information relates to employment or educational history*
> […]

[…]

(g) the personal information consists of the third party's name when

(i) it appears with other personal information about the third party, or

(ii) the disclosure of the name itself would reveal personal information about the third party,

[…]

(5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether

(a) the disclosure is desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny

(b) the disclosure is likely to promote public health and safety or the protection of the environment,

(c) the personal information is relevant to a fair determination of the applicant's rights,

(d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people,

(e) the third party will be exposed unfairly to financial or other harm,

(f) the personal information has been supplied in confidence,

(g) the personal information is likely to be inaccurate or unreliable,

(h) the disclosure may unfairly damage the reputation of any person referred to in the record requested by the applicant, and

(i) the personal information was originally provided by the applicant.

[para 17] Section 17 does not say that a public body is never allowed to disclose third party personal information. It is only when the disclosure of personal information would be an unreasonable invasion of a third party's personal privacy that a public body

must refuse to disclose the information to an applicant under section 17(1). Section 17(2) establishes that disclosing certain kinds of personal information is not an unreasonable invasion of personal privacy.

[para 18] When the specific types of personal information set out in section 17(4) are involved, disclosure is presumed to be an unreasonable invasion of a third party's personal privacy. To determine whether disclosure of personal information would be an unreasonable invasion of the personal privacy of a third party, a public body must consider and weigh all relevant circumstances under section 17(5), (unless section 17(3), which is restricted in its application, applies). Section 17(5) is not an exhaustive list and any other relevant circumstances must be considered.

Reasons for being away from the office

[para 19] The Public Body withheld information regarding employees' reasons for being out of the office. An employee's personal reasons for being out of the office are the employee's personal information falling within the terms of section 17(4)(1)(g). Section 17(4) deems it to be an unreasonable invasion of an individual's personal privacy to disclose information falling within its terms. On the evidence before me, there are no factors weighing in favor of disclosing this information and so I will confirm the Public Body's decision to sever information regarding employee absences.

Extension numbers and room / workstation numbers

[para 20] The Public Body severed information from an organizational chart and directory. The severed information includes photographs and names of employees, their job duties, titles, office numbers and extension numbers. These records are responsive to the access request as the Applicant's name appears in them.

[para 21] In Order F2019-09, the Adjudicator found that the direct line numbers of employees in a public body's internal telephone directory were not personal information to which section 17 may be applied. She said:

> Ontario's *Freedom of Information and Protection of Privacy Act* excludes business contact information from the definition of personal information (section 2). In Ontario Order PO-3055 considered whether work cell phone numbers are personal information. The adjudicator noted that unlike business phone numbers or home phone numbers, "cell phone numbers can be ambiguous as to whether they represent the individual in their personal or professional capacity. In some circumstances, an individual can use a cell phone number in both contexts" (at para 243). She concluded (at para. 244):
>
> > In my view, where a cell phone number appears in a business context, together with an individual's professional information, inviting one to contact the individual in a professional capacity as they do in the current appeal, it cannot be said to qualify as personal information within the meaning of that definition in section 2(1) of the *Act*.

> Rather, the cell phone number[s], as they appear in the records at issue, are more accurately described as professional or business information as contemplated by section 2(3) of the *Act*.

The Public Body has also argued that the Skype system allows employees to make contact via instant messaging and video, which adds a personal dimension to the phone number. I do not see how the ability to message or text a work-issued cell phone number adds a personal dimension *to the phone number*. If the phone kept a recording of the employee's video calls, there may be recorded personal information of the employee (even if the video call were work-related). In that case, the personal information would be the video, not the phone number. The fact that a phone has video capabilities does not add a personal dimension to the assigned phone number. Further, how an employee uses a cell phone may have a personal dimension, but the work-assigned phone number alone does not.

Employer-issued cell phone numbers (or landline numbers, for that matter) could reveal personal information about an employee if that number was associated with other personal information of the employee. For example, phone logs that reveal personal calls made by the employee to a medical specialist may constitute personal information. However, it is not the number that is personal information; the personal information is the fact that the individual contacted that medical specialist. In some circumstances, the employer-issued phone number might not be severable from the personal information, in which case it could reveal personal information as well.

In this case, as the Public Body has pointed out, there is no such context that could add a personal dimension to the phone numbers. The phone numbers appear in a directory and provide no additional information about the employees to whom they are assigned.

The phone numbers in the staff directory, whether assigned to landlines or cell phones, are assigned to the Public Body employees for the purpose of being contacted for their work. Nothing in the Public Body's submissions satisfies me that these numbers have a personal dimension such that section 17(1) could apply. Regarding cell phone numbers, I prefer the analysis from Order F2018-36 and the Ontario orders: the fact that an employee may use an employer-issued cell phone to make a personal call, or that the employee may carry the cell phone with them, does not alter the character of the work-issued cell phone *number* such that it has a personal dimension. Employees may also use landlines to make personal calls, or employer-issued email addresses to send personal emails; the occasional personal use of a work-issued phone or email address does not make the phone number (or email address) the personal information of the employee.

[para 22] In that Order, the Adjudicator found that a public body's directory of the business contact information of employees was not personal information to which section 17(1) could be applied. I find the same holds true for the extension numbers in the directory on records 450 – 451.

[para 23] For the same reasons, I find that the office numbers assigned to employees are also not the employees' personal information to which section 17 may be applied. The offices are where employees perform work on behalf of the public body; the number assigned by the public body to an employee's workstation or office, without more, lacks a personal dimension.

[para 24] In *Edmonton (City) v Alberta (Information and Privacy Commissioner)*, 2016 ABCA 110 (CanLII), the Court of Appeal confirmed that personal information requires a "personal dimension", and stated:

> In general terms, there is some universality to the conclusion in ***Leon's Furniture*** that personal information has to be essentially "about a person", and not "about an object", even though most objects or properties have some relationship with persons. As the adjudicator recognized, this concept underlies the definitions in both the *FOIPP Act* and the *Personal Information Protection Act*. It was, however, reasonable for the adjudicator to observe that the line between the two is imprecise. Where the information related to property, but also had a "personal dimension", it might sometimes properly be characterized as "personal information". In this case, the essence of the request was for complaints and opinions expressed about Ms. McCloskey. The adjudicator's conclusion (at paras. 49-51) that this type of request was "personal", relating directly as it did to the conduct of the citizen, was one that was available on the facts and the law.

[para 25] The direct lines and office numbers in this case indicate how to contact employees for work-related purposes and lack a personal dimension. As a result, are not personal information to which section 17(1) can apply.

Job titles, employee names, photographs, duties

[para 26] The Public Body applied section 17(1) to withhold:

> […] people's names along with other information such as their new or previous job titles, phone numbers (which may not necessarily be available to the public), office location, employment position, etc. Section l(n)(I) of the *FOIP Act* defines personal information as "recorded information about an identifiable individual, including the individual's name, home or business address or home or business telephone number".
>
> The disclosure of the personal information is an unreasonable invasion of a third party's personal privacy. Section 17(4)(g)(i) of the FOIP Act states that "a disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if the personal information consists of the third party's name when it appears with other personal information about the third party". In this case, the information includes people's new or previous job titles, phone numbers (which may not necessarily be available to the public), office location, employment position, etc.

[para 27] Section 17(4)(d) creates a presumption that disclosure of personal information relating to employment history is an unreasonable invasion of personal privacy. In order F2004-026, former Commissioner Work adopted the following interpretation of the phrase "employment history," as set out in Order F2003-005:

> In my view the term 'employment history' describes a complete or partial chronology of a person's working life such as might appear in a resume or personnel file. Particular incidents that occur in a workplace may become the subject of entries in a personnel file, and such entries may properly be

> viewed as part of 'employment history'. However, the mere fact there is a written reference to or account of a workplace event does not make such a document part of the 'employment history' of those involved. Many workplace incidents of which there is some written record will not be important enough to merit an entry in a personnel file.

Former Commissioner Work considered employment history within the terms of section 17(4)(d) to refer to information of an employee's personal work history, such as would be found in a human resources file. Examples would be records of workplace discipline or investigations involving the employee. Another example would be an employee's resume, which contains a record of an employee's personal work and education history.

[para 28] I am unable to identify any information falling within the terms of section 17(4)(d) in the records at issue. Rather, the majority of information severed by the Public Body falls within the terms of section 17(2)(e).

[para 29] Section 17(2)(e) applies to personal information such as the employee's classification, job description, and employment duties as an employee of a public body. The Public Body severed personally identifying information of employees and their job titles and responsibilities, from records 178, 179, 181, 448 – 450 and 450 – 451 under section 17(1). However, such information is personal information falling under section 17(2)(e) and cannot be withheld under section 17, as section 17(2) of the FOIP Act deems disclosure of such information not to be an invasion of personal privacy. While the Public Body argues that the information about classifications is historical, there is nothing in the records that indicates this. In addition, section 17(2)(e) does not distinguish between old information about classifications and new. If information about an employee's former classification is contained in the employee's résumé, I would agree that section 17(4)(d) could apply, as that constitutes an employee's employment history. However, the information about classifications in the records before me is not about employee's employment histories, but is intended to establish which employees in various teams hold particular classifications and responsibilities at the time the records were created. As a result, section 17(2)(e) applies.

[para 30] That section 17(2)(e) applies to "personal information" also means that it applies to personally identifying information that regarding the holder of the job description, title, or classification. For example, the entire sentence, "Jane Doe is the Manager of Communications" would be subject to section 17(2)(e), as the personal information in this sentence is that Jane Doe is the holder of the work title and classification. If section 17 contemplated that Jane Doe's name should be severed, there would be no need for section 17(2)(e), as a classification in the absence of personally identifying information is not personal information about an identifiable individual.

[para 31] I note that the organizational chart in the records also contains photographs of managers, in addition to their names. It appears that this chart may be intended to ensure that new staff members are able to identify senior team members to

understand who to speak to and report regarding work-related matters. In any event, the photograph serves the same purpose as a name in the context of the information regarding job titles and work duties: it informs the reader of the identity of the holder of a particular position. The photograph is personal information, as are the names of employees, but in the context of information subject to section 17(2)(e).

[para 32] Like a name, a photograph arguably conveys something about an individual outside the workplace. As noted above, section 17(2)(e) acknowledges that the information it deems not to result in an invasion of personal privacy if disclosed, may be personal information.. Both the names and the photographs in the records are intended to inform the reader of the identity of the holders of various positions and titles in the Public Body's organization. I find that the names and photographs are both subject to section 17(2)(e).

Safety

[para 33] In its rebuttal submissions, the Public Body argued the following:

> These personal information redactions are not just professional/business in nature, but have a personal or safety element to them. The 17(1) redactions include:
>
> - names of staff who missed work;
> - changes in staffing roles (including past roles held and names of former staff who held the position);
> - staff's new/previous job titles and employment position; and
> - specific office room numbers of staff and phone numbers (which may only be shared internally).

[para 34] The Public Body refers to concerns regarding safety if the information it severed under section 17 is disclosed. Section 18 of the FOIP Act authorizes a public body to sever information if the public body reasonably believes that disclosure could undermine safety. It states, in part:

> *18(1) The head of a public body may refuse to disclose to an applicant information, including personal information about the applicant, if the disclosure could reasonably be expected to*
>
> *(a) threaten anyone else's safety or mental or physical health, or*
>
> *(b) interfere with public safety.*

[para 35] There can be overlap between section 17, as in the situation where severing an individual's personal information may protect the individual's personal privacy in addition to ensuring that the individual's safety is not threatened.

[para 36] In Order F2013-51, the Director of Adjudication reviewed past orders of this office regarding the application of section 18. She said:

> These cases establish that section 18 of the FOIP Act applies to harm that would result from disclosure of information in the records at issue, but not to harm that would result from factors unrelated to disclosure of information in the records at issue. Further, a public body applying section 18 of the FOIP Act must provide evidence to support its position that harm may reasonably be expected to result from the disclosure of information (as must a custodian applying section 11(1)(a) of the HIA).
>
> Following the approach adopted by the former Commissioner in Order 96-004, and in subsequent cases considering either section 18 of the FOIP Act or section 11 of the HIA, the onus is on the Public Body to provide evidence regarding a threat or harm to the mental or physical health or safety of individuals, to establish that disclosure of the information and the threat are connected, and to prove that there is a reasonable expectation that the threat or harm will take place if the information is disclosed.

[para 37] The Public Body has not explained how harm would be likely to result from the disclosure of the information it severed under section 17(1). Without evidence or argument as to the anticipated harm, I am unable to find that anyone's safety would be threatened by disclosure of this information.

[para 38] Recently, in Order F2021-28 I determined that information such as cell phone numbers and direct lines may be withheld under section 25, if there is evidence that the Public Body will likely have to expend funds to change the numbers if they become public. I said:

> Although I do not agree with the Public Body's application of section 17 and 20(1)(m) to cell phone numbers and direct lines of police officers and Crown prosecutors, I believe that there is an exception in the FOIP Act that enables public bodies -- not only those involved in law enforcement -- to sever cell phone numbers and direct lines from records for the reasons I have discussed above: the concern that making the number public will render it unusable because of the likelihood that it will receive too many calls for the employee to reasonably answer, or be used by individuals who should not contact an employee directly, due to the nature of the employee's employment. If it can be anticipated that once a cell phone or direct line is made public, the public body will likely have to assign a new number, then section 25 of the FOIP Act applies to the number.
>
> […]
>
> Section 25 will apply to the telephone numbers assigned to a public body's employee if it can reasonably be expected that the Public Body will need to change the employee's telephone number once it has been provided to an applicant / made public through an access request. Evidence as to the reasons why a public body restricts access to the number, how it treats the employee's calls, the public body's organizational structure and purpose, and the employee's work duties, will be necessary to establish the application of section 25.

[para 39] In this case, I am unable to conclude that there would be any increase in calls to the extensions of employees if the extension numbers were released, or that

employees would be likely to receive calls that could compromise the Public Body's activities, given that the evidence I have regarding the employees' work duties does not suggest a likelihood that this could reasonably be expected to happen.

Summary

[para 40] As discussed above, I accept that reasons why employees miss work have a personal dimension and is information that may be severed under section 17(1) in the absence of factors weighing in favor of disclosure. I will confirm the Public Body's decision to sever this information. For the reasons above, I find that section 17(1) does not require the Public Body to sever the remaining information to which it applied this provision and I must direct it to disclose it.

ISSUE C: Did the Public Body properly apply section 24(1) of the Act (advice from officials) to the information in the records?

[para 41] Section 24 states, in part:

> *24(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to reveal*
>
> > *(a) advice, proposals, recommendations, analyses or policy options developed by or for a public body or a member of the Executive Council,*
> >
> > *(b) consultations or deliberations involving*
> >
> > > *(i) officers or employees of a public body,*
> > >
> > > *(ii) a member of the Executive Council, or*
> > >
> > > *(iii) the staff of a member of the Executive Council […]*
>
> *(2) This section does not apply to information that*
>
> > *[…]*
> >
> > *(b) is a statement of the reasons for a decision that is made in the exercise of a discretionary power or an adjudicative function,*
> >
> > *[…]*
> > *(f) is an instruction or guideline issued to the officers or employees of a public body,*

> *(g) is a substantive rule or statement of policy that has been adopted by a public body for the purpose of interpreting an Act or regulation or administering a program or activity of the public body.*

[para 42] In Order F2015-29, the Director of Adjudication interpreted sections 24(1)(a) and (b) of the FOIP Act and described the kinds of information that fall within the terms of these provisions. She said:

> The intent of section 24(1)(a) is to ensure that internal advice and like information may be *developed* for the use of a decision maker without interference. So long as the information described in section 24(1)(a) is developed by a public body, or for the benefit or use of a public body or a member of the Executive Counsel, by someone whose responsibility it is to do so, then the information falls under section 24(1)(a).
>
> A consultation within the terms of section 24(1)(b) takes place when one of the persons enumerated in that provision solicits information of the kind subject to section 24(1)(a) regarding that decision or action. A deliberation for the purposes of section 24(1)(b) takes place when a decision maker (or decision makers) weighs the reasons for or against a particular decision or action. Section 24(1)(b) protects the decision maker's request for advice or views to assist him or her in making the decision, and any information that would otherwise reveal the considerations involved in making the decision. Moreover, like section 24(1)(a), section 24(1)(b) does not apply so as to protect the final decision, but rather, the process by which a decision maker makes a decision.

[para 43] I agree with the analysis of the Director of Adjudication as to the purpose and interpretation of sections 24(1)(a) and (b), and agree these provisions apply to information generated when a decision maker asks for advice regarding a decision, or evaluates a course of action

[para 44] The Applicant argues:

> I cannot judge whether the public body applied section 24(1) properly because this information was blacked out and I could not see it. I trust the adjudicator will make their decision based on the FOIP Act. I would like to add that section 24 (2) (b, f, g) describe situations where section 24(1) doesn't apply and they should be examined carefully.

[para 45] The Public Body states in its reply submissions:

> The redacted portions are not made in the exercise of a discretionary power or an adjudicative function, not an instruction or guideline issued to the officers or employees of a public body, nor could they be considered a substantive rule or statement of policy that has been adopted by a public body for the purpose of interpreting an Act or regulation or administering a program or activity of the public body.
>
> ECSD maintains that the redactions pass the test for what should be considered as advice, recommendations, consultations and/or deliberations

[para 46] I reviewed the information the Public Body severed and agree that it falls within the terms of section 24(1) and not 24(2). The severed information consists of analysis and discussion of the pros and cons of courses of an action under consideration.

[para 47] I also find that the Public Body appropriately exercised its discretion when it severed information under section 24(1). The purpose of section 24(1) is to ensure that a public body's employees may give frank advice without interference and that this purpose is served by withholding the information from the Applicant. On the evidence before me, I am unable to identify any significant interests that would be served by disclosing the information.

IV. ORDER

[para 48] I make this Order under section 72 of the Act.

[para 49] I confirm that the Public Body met its duty to assist by conducting an adequate search for responsive records.

[para 50] I confirm the Public Body's decision to withhold information from the Applicant under section 24(1).

[para 51] I confirm the Public Body's decision to sever personal information regarding employee absences from the records under section 17(1). I order the Public Body to give access to the Applicant to the remaining information to which it applied section 17(1).

[para 52] I order the Public Body to inform me within 50 days of receiving this order that it has complied with it.

_____

Teresa Cunningham
Adjudicator
/bah