Procedure Title	**Employee Personal Information and Medical Records – Collection and Use**		
Date of Issue	May 26, 2021 (formerly AP2350-D and AP 7215-D)	**Related Policy**	BP 1408-D
Revision Dates		**Related Forms**	
Review Date		**Originator**	Administrative Council
References			
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA); Ontario Employment Standards Act (ESA); Information and Privacy Commissioner of Ontario Fact Sheet "Communicating Personal Health Information by Email", September 2016; Workplace Safety and Insurance Act			

1.0 RATIONALE

1.1 The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) specifies how personal information can be collected and accessed. It is therefore the board's responsibility to safeguard the confidentiality of personal information pertaining to its staff.

1.2 The Employment Standards Act dictates that all employers in Ontario are required to keep written records about each person they hire.

2.0 PROCEDURE

2.1 Collection and Use

2.1.1 Personal information will be collected in accordance with the MFIPPA. All personal information will be kept safe, and confidentiality will be protected by each employee who is authorized to have access to this information for the purposes of human resources services and/or employee administration. Only those employees who require access to perform their assigned job function will have access to the personnel file.

2.1.2 Access to an employee's personnel file can be obtained during normal working hours and is available to:

a. authorized persons as in section 2.1.1;

b. the employee (with appropriate notice and supervision); and

c. other parties with the specific written consent of the employee (with appropriate notice and supervision).

2.1.3 Copies of personal information will be provided only with the specific written consent of the employee. A record of all such transactions must be kept in the employee's file. Section 32 of the MFIPPA exempts the need for employee consent for disclosure of personal information if it is to a law enforcement agency, or if the release is to comply with another Act, or in compelling circumstances affecting the health and safety of an individual. Additionally, section 52 (3) of the MFIPPA excludes certain documents from disclosure, such as:

2.1.3.1 Proceedings or anticipated proceedings before a court, tribunal or other entity relating to labour relations or to the employment of a person by the institution.

2.1.3.2 Negotiations or anticipated negotiations relating to labour relations or to the employment of a person by the institution between the institution and a person, bargaining agent or party to a proceeding or an anticipated proceeding.

2.1.3.3 Meetings, consultations, discussions or communications about labour relations or employment related matters in which the institution has an interest.

2.2 Maintenance of Employee Records

2.2.1 Employee records and personal information will be maintained by the Human Resources Services Department in a secure area. This area will be accessible only through a coded entry system. Only persons who require access to these records in the performance of their respective job function will have access.

2.2.1.1 Electronic access to employee information will be password protected.

2.2.2 Confidential information retained in an employee's file located at the Bluewater District School Board Education Centre will be placed in one or more sealed envelopes. This includes, but may not be limited to:

a. Performance evaluations (probationary employees, upon employee request, employee whose performance requires evaluation, Annual Learning Plan during an evaluation year)
b. Disciplinary letters (in accordance with collective agreements)
c. Benefit coverage selection and payroll deductions

2.2.3 A secondary file may be retained in the work location, i.e. schools by the worksite administrator (principal/supervisor). The secondary file is to be maintained and accessed in the same manner as the primary personnel file. A secondary file will contain minimal records; that is, only those records that relate to a board employee that a principal/supervisor "needs to know" to perform their supervisory responsibilities.

2.2.4 When the employee is transferred to another school/workplace within the board, the employee's secondary file shall be forwarded to the administrator/supervisor of the new work site or to the Human Resources Services Department, Bluewater District School Board Education Centre.

2.3 Employee Medical / Workplace Safety and Insurance Board (WSIB) Information

2.3.1 Employee medical information should be forwarded, in an expeditious and confidential manner, directly to the superintendent of education responsible for human resources services, or designate, where it will be maintained in the strictest confidence. The employee should keep a copy of the information for their own files.

2.3.1.1 If the principal/supervisor receives medical information from an employee, they will forward it, in an expeditious and confidential manner, directly to the superintendent of education responsible for human resources services, or designate, and destroy any copies that they have remaining in their file.

2.3.2 Employee medical information must not be kept in the employee's secondary file.

2.3.3 Employee medical records and Workplace Safety and Insurance Board of Ontario (WSIB) records, whether active or in storage, are maintained separately from the employee's personnel file in the Human Resources Services Department.

2.3.4 The superintendent responsible for human resources services, or designate, is solely responsible for all employee medical records and WSIB claim records and is the only person who shall have access to these records. The WSIB claim records may consist of non-medical and medical records and these shall be handled in a manner consistent with the provisions of the Workplace Safety and Insurance Act and the MFIPPA, where applicable.

2.3.5 An employee may request information contained in their medical file by contacting superintendent responsible for human resources services or designate. Photocopies of specific information shall be given to the employee upon written request.

2.3.6 No information from an employee's medical records is given to a third party without the employee's written consent, unless required by law. If required by law, the superintendent responsible for human resources services, or designate, shall notify the employee.

2.3.7 The confidential nature of all personal and medical information provided by the employee or their treating practitioner(s) to the school board will be respected by all involved parties.

2.3.8 If medical information must be sent electronically, it **must** be deleted from individual fax or email inboxes, and email recycle bins, after it has been sent to the Human Resources Services Department, ensuring that the proper electronic/email deletion schedule can be applied. It is only advisable to share confidential medical information by email when encryption is available. If encryption is not available, or cannot be guaranteed, then the sender should evaluate whether it is reasonable to communicate via unencrypted electronic means. The following, from the Information and Privacy Commissioner of Ontario Fact Sheet "Communicating Personal Health Information by Email", September 2016, should be utilized to consider whether it is reasonable to communicate through unencrypted email:

2.3.8.1 **Characteristics of the Information**
What type of information is being communicated? While all personal information is sensitive, the degree of sensitivity can vary. For example, the time and date of an appointment may not be as sensitive as diagnostic information contained in an individual's health record.

2.3.8.2 **Volume of Information and Frequency of Correspondence**
As the volume and frequency of emails increases, so does the risk. Will the email include a large volume of personal health information? Is the information being sent only one time, or on a frequent or continuous basis?

2.3.8.3 **Purpose of the Transmission**
Is email only being used for administrative purposes (e.g., appointment reminders, providing general health resources)?

2.3.8.4 **Patient (employee's) Expectations**
What is the patient/employee's expectations as to how the information will be communicated?

2.3.8.5 **Availability of Alternative Methods and their Associated Risks**
What are the available alternative methods of communication? Each method should be assessed for risks to privacy and confidentiality and select the method that poses a risk level that is proportional to the harm that could result from a privacy breach.

2.3.8.6 **Emergency and Other Urgent Circumstances**
Is unencrypted email the timeliest and most practical means to communicate the information to the individual and/or prevent harm?

2.3.9 After considering the factors noted in section 2.3.8, the sender must be satisfied that the use of unencrypted email is reasonable. If not satisfied that it is reasonable, then the information should not be communicated unencrypted. Consent must be obtained from the patient/employee prior to the use of unencrypted email.

2.3.10 Similar considerations to those noted in section 2.3.8 will be reviewed when handling general personal / employee information by email.

2.4 Retention/Destruction

Employee personal and medical information that is no longer required may be destroyed in a confidential manner in accordance with relevant legislation, the board's classification and retention schedule, and WSIB legislation, where appropriate.