## 1. GENERAL

**1.1** The transfer or placement of students shall be in accordance with the Manitoba Pupil File Guidelines, the Public Schools Act, The Education Administration Miscellaneous Provisions Regulation, The Freedom of Information and Protection of Privacy Act (FIPPA), The Personal Health Information Act (PHIA), The Youth Criminal Justice Act (Canada) and The Adoptions Act, and applicable legislation including Division Policies.

In accordance with the Public Schools Act, for greater certainty, nothing in sections 42.1 to 42.5 shall be interpreted to restrict the ability of a school board or a person acting on behalf of a school board to disclose information contained in a pupil file, provided the disclosure is made in good faith and within the scope of the duties and responsibilities of the school board or the person.

The Protecting Children (Information Sharing) Act allows government departments, organizations and others who provide services to at-risk and vulnerable children to collect, use and share personal information, including personal health information, about supported children and their parents or legal guardians. Personal information can be shared without consent, only when it is in the best interests of a supported child.

## 2. RESPONSIBILITIES

### 2.1 Chief Superintendent/CEO

The Chief Superintendent or designate shall authorize the transfer or placement of students.

### 2.2 Principal

The principal shall inform the parent/guardian when a transfer or placement in another school is being considered by the school, unless prevented by other legislation.

**2.2.1** In accordance with the Manitoba Pupil File Guidelines, the principal shall forward the pupil file, including the cumulative components and all files which comprise the support file component, when the student transfers out of the school and enrols in another.

**2.2.2** The contents of the pupil file being transferred should be reviewed to ensure that only personal information and personal health information necessary for the schooling and provision of educational services to the student is forwarded to the new school.

**2.2.3** The youth criminal justice component of the pupil file may not be transferred from one school to another within a school division, nor transferred to a school within a different school division. In that case, the youth criminal justice component of a pupil file must be destroyed.

**2.2.4** The transfer procedures should ensure that the file contents, as they are of a sensitive and personal nature, are adequately protected from unauthorized access, disclosure, loss or destruction while being transferred.

**2.2.5** The pupil support file component should be transferred directly from administrator to administrator wherever possible to further ensure the security and confidentiality of the file contents.

**2.2.6** When a student enrolled in a school is placed for adoption, a new pupil file for the student's adoptive identity must be created before the pupil file is transferred to the student's new school.

## 3. PRIVACY

At all times during this process, the file(s) must be adequately protected from unauthorized access, disclosure, loss or destruction.

## 4. BREACH

As outlined in the Division's Policy, Access & Privacy, a Breach of Privacy occurs when Personal Information, including Personal Health Information, is collected, accessed, used, disclosed, transported, transmitted, transferred or destroyed other than as authorized, or when the accuracy, confidentiality or integrity of the information is compromised and therefore is in violation of PHIA. Breaches may include, but are not limited to, the viewing of Confidential Information by unauthorized individuals, the access, theft or loss of Division Records and the unauthorized destruction of such information by deliberate means or by human or natural accident.

### 4.1 All breaches are required to be reported immediately to the Access and Privacy Coordinator.

(a) Any Person Associated with the Division who becomes aware of a possible or actual Breach of Privacy, shall immediately report the possible or actual Breach of Privacy to the Access and Privacy Officer and/or Coordinator, who shall take immediate steps to contain the Breach.
(b) All Breaches of Privacy will be investigated by the Access and Privacy Officer and Coordinator.
(c) The Access and Privacy Officer and Coordinator will make recommendations for immediate and long-term corrective measures as necessary to protect the confidentiality, integrity and security of all Personal Information and Personal Health Information.
(d) If it is determined that a Breach of Privacy has occurred, appropriate remedial action shall be taken by the Division. Such action may include disciplinary action, which will be implemented pursuant to and in accordance with the relevant collective agreement, Division policies or by-laws.
(e) The Access and Privacy Officer and Coordinator will act as a resource for all persons associated to the Division regarding appropriate action to be taken following a Breach of Privacy.