情報セキュリティポリシー

大正小学校

１　目的

教育活動の充実と効率的な校務処理を目指して情報化を推進するにあたり、児童・生徒、保護者、教職員等、本校関係者の個人情報をはじめとする情報資産を情報リスクから守り、信頼される教育の実現のための総合的な情報セキュリティを実施する。

２　学校の責務

（学校の責務）

（１）学校における情報管理の責任を明確化するとともに、教職員の責務を規定する。

（２）　情報セキュリティに関する法令等を全教職員に周知徹底し、情報資産の適切な管理を行う。

（教職員の責務）

（３）教職員は、目的に定める基本理念及び情報セキュリティの重要性について認識し、情報資産を適切に取り扱わなければならない。

（４）教職員は、情報資産の取扱いに当たっては、次に掲げる法令等を遵守しなければならない。

（ア）学校における生徒等に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針（文科省告示１６１号）

（イ）横浜市個人情報の保護に関する条例（平成 17 年２月横浜市条例第６号）

（ウ）横浜市教育委員会情報セキュリティ管理規程

（エ）横浜市教育委員会情報セキュリティ管理要綱

（オ）横浜市教育委員会情報セキュリティ対策共通実施手順

（カ）横浜市教育委員会情報セキュリティ管理に係る取扱要領

（キ）横浜市立学校における個人情報の取扱いについて（通知）（令和３年１月）

（情報セキュリティ担当者及び情報資産管理者等の設置）

（５）目的を達成するため、学校内に情報セキュリティ担当者及び情報資産管理者、情報管理担当者を置く。

（６）情報セキュリティ担当者及び情報資産管理者に、学校長をあてる。

（７）情報管理担当者に、情報担当者をあてる。

３　情報セキュリティ担当者

（１）教職員に対し、情報資産の取扱いに関する校内研修を実施する。

（２）情報セキュリティ対策の実施状況についての点検を定期的に行う。

（３）ウイルス等による被害が発生した場合には、速やかにウイルス等対策窓口あてに報告する。

（４）事故対応に備え、情報セキュリティ事故対応手順に基づき、定期的に訓練を実施する。

４　情報資産管理者

情報資産管理者は情報管理担当者ならびに教職員を総括し、これらの者に対し情報セキュリティに関する事項の指示及び指導・監督を行う。

（情報資産の管理）

（１）　教職員のデータへのアクセス制限及び利用者の認証に関する管理を行う。

（２）　情報資産の校外持ち出しを原則禁止とする。

（３）　情報資産は必ず鍵のかかる場所で保管する。

（４）　端末機等はセキュリティワイヤーで固定するか、鍵のかかる室内や保管庫等により、盗難防止対策を行う。

（５）　記録媒体等が不要になった場合、情報を復元できないように処置したうえで廃棄する。

（６）　必要な端末機及び電磁記録媒体等を確保し、管理する。

（７）　記録媒体について、必要に応じて定期的にバックアップを行う。

（８）教職員からデータを紛失、漏えい、消失した報告を受けた場合には、情報資産管理者は速やかに次のことを行う。

（ア）各方面の学校教育事務所に報告する。

（イ）漏えい情報の回収及び謝罪等を行う。

（８）　データの保存状況について、定期点検を行う。

（情報管理担当者の責務）

情報管理担当者は、情報セキュリティ担当者及び情報資産管理者を補佐するとともに、教職員への情報セキュリティ対策の実施の徹底を図るため、学校の情報資産を利用する教職員に対して指示及び指導を行う。

５　実施手順書（教職員一人ひとりが守るべき事柄）

（１）端末機及び記録媒体は、原則学校保有のものを使用する。ただし、緊急時で情報セキュリティ担当者が認めた場合については、 学校保有以外の端末機を使用することができる。その際は、取扱う情報の範囲を限定し、承認されたクラウドサービスで行うこと。

（２）端末機の使用にあたっては、次のことを確認する。

（ア）セキュリティ対策ソフトウェア が最新の 状態に 更新されていること 。

（イ）0S やアプリケーションソフトウェアが最新の状態に更新 されていること 。

（ウ）アプリケーションソフトウェアは正規のライセンスのものを使用していること。

（３）端末機の画面の向きに注意し、離席時に他人から容易に見られないようログイン状態にならないようにする。

（４）データの校外持ち出しは禁止とする。

（５）データを校外に持ち出す必要性が生じた場合には、次の点を厳守する。

(ア)「個人情報校外持ち出し簿」に必要事項を記入し、必ず情報資産管理者の許可を得る。

(イ)第三者に読み取られないよう、データの暗号化を必ず行う。

(ウ)持ち出し先で使用する場合は、次のことを厳守する。
・最新のセキュリティ対策ソフトウェアで、セキュリティチェックが行われていること。
・本体ハードディスク内及びデータを残さないこと。
（６）持ち出した記録媒体を返却する場合は、次のことを厳守すること。
（ア）)最新のセキュリティ対策ソフトウェアでセキュリティチェックを行った上で、サーバ等にデータを保管する。
(イ)記録媒体のデータを完全に消去する。
(ウ)「個人情報校外持ち出し簿」に必要事項を記入し、情報資産管理者等に返却する。
(エ）原則、即日返却する。
（７）データを紛失、漏えい、消失した場合には、教職員は、情報資産管理者に直ちに報告する。
（８）ウイルス等に感染した場合は、直ちにネットワークから切り離し、情報資産管理者に報告する。