松川町教育情報セキュリティポリシー
【基本方針】

令和８年３月改定
松川町教育委員会

第１章　教育情報セキュリティ基本方針

第１条　目的

松川町の各小中学校で使用する情報資産には、生徒・児童の個人情報をはじめ学校運営に必要な情報など、部外に漏洩、あるいは滅失した場合には極めて重大な結果を招く情報が多数含まれている。これらの情報資産を人的脅威や災害、事故等から防御することは、生徒・児童及び教職員の財産、プライバシーを守るためにも、また、継続的かつ安全・安定的な学校運営の確保のためにも必要不可欠である。

また、近年、情報教育において、情報モラルや情報セキュリティにも重点が置かれる中で、学校がその模範を示すことは、生徒・児童への指導の上で非常に重要なことであり、そのためには、情報資産が安全に保護管理されること、およびネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件となる。

このため、各学校の情報資産の機密性、完全性及び可用性を維持するための対策を整備することを目的として、松川町小中学校教育情報セキュリティポリシーを定め、情報セキュリティの確保に最大限取り組むものである。

このうち教育情報セキュリティ基本方針は、松川町の小中学校が保有する教育情報資産の機密性、完全性及び可用性を維持するため、各学校が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

第２条　用語の定義

（１）電子計算機

ハードウェア及びソフトウェアで構成するコンピュータ、及び周辺機器並びに記録媒体（磁気ディスク等並びに入出力帳票及び情報システム仕様書等）をいう。

（２）ネットワーク

電子計算機を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）で構成され、情報処理を行う仕組みをいう。

（３）情報システム

松川町の小中学校の各種電子計算機（ネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

（４）情報資産

ネットワーク及び情報システム並びにそれらの開発と運用に係る全てのデータ並びにネットワーク及び情報システムで取り扱う全てのデータ、並びに職務で使用する電子機器、電磁的及び光学的記録、書類、帳票等をいう

（５）情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（６）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（７）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（８）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（９）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(10) 校務系

児童生徒の成績、指導要録、教員の個人情報等に係る情報システム及びデータをいう。

(11) 教職員

松川町の小中学校に勤務する全ての職員（非常勤職員及び臨時的任用職員を含む）をいう。

(12) 外部委託者

職務委託先社員等、契約に基づいて松川町の小中学校で作業する者の総称をいう。

(13) 部外者

教職員、町職員、及び外部委託者以外の松川町の小中学校の情報資産に接

することが認められていない者の総称をいう。

（14）不正アクセス

不正アクセス行為の禁止等に関する法律（平成１１年法律第 128 号）第３条第２項に規定する不正アクセス行為その他の不正な手段により利用者以外の者が行うアクセス又は利用者が行う権限外のアクセスをいう。

第３条　情報セキュリティポリシーの位置付け

情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、松川町の小中学校が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

第４条　教育情報セキュリティポリシーの対象範囲

教育情報セキュリティポリシーの適用範囲は、次の各項に定めるものとする。

（１）適用資産

本ポリシーの対象資産は、松川町の小中学校における全ての情報資産とする。ただし、松川町情報セキュリティポリシーの適用対象となる資産は、本ポリシーの適用対象外とする。

（２）適用対象者

教育情報セキュリティポリシーの適用対象者は、前項に示す情報資産に接する全ての教職員及び教育委員会職員とする。

第５条　教職員の義務

松川町の小中学校が所掌する情報資産に関する業務に携わる全ての教職員及び教育委員会職員は、情報セキュリティの重要性について共通の認識をもつとともに職務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

第６条　情報資産への脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を

実施する。

（１）部外者の侵入による機器又は情報資産の破壊、盗難、不正アクセス、コンピュータウィルス攻撃、サービス不能攻撃等の意図的な要因による機器又は情報資産の漏えい、破壊、盗聴、改ざん、消去等。

（２）教職員、教育委員会職員及び外部委託者による機器又は情報資産の無断持ち出し・誤操作、アクセスのための認証情報又はパスワードの不適切管理、規定外の端末接続や無許可ソフトウェアの使用等の規定違反、プログラム上の欠陥、搬送中の事故等による機器又は情報資産の盗難、故障等の非意図的要因による情報資産の漏えい、破壊、消去等。

（３）地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止。

第７条　情報セキュリティ対策

小中学校の教育情報資産を第６条に示した脅威から保護するために、以下の情報セキュリティ対策を講じるものとする。

（１）組織体制
小中学校の情報資産について、情報セキュリティ対策を推進・管理するための体制を確立するものとする。

（２）情報資産の分類と管理
小中学校が保有する情報資産をその重要度に応じて分類し、当該分類に基づき情報セキュリティ対策を行うものとする。

（３）物理的セキュリティ対策
サーバ等、職員室、教室等、通信回線等及び教職員のパソコン等、書類等の管理について、物理的な対策を講じる。

（４）人的セキュリティ対策
情報セキュリティに関し、教職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（５）技術的セキュリティ対策

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（６）運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

第８条　情報セキュリティ監査及び自己点検の実施

教育情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

第９条　教育情報セキュリティポリシーの見直しの実施

情報セキュリティ監査及び自己点検の結果等により、教育情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、教育情報セキュリティポリシーの見直しを実施する。

第１０条　教育情報セキュリティ対策基準の策定

小中学校の様々な情報資産について、第７～９条に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める教育情報セキュリティ対策基準を策定する。

第１１条　教育情報セキュリティ実施手順の策定

教育情報セキュリティ対策基準に基づき、教育情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

第１２条　教育情報セキュリティポリシーの情報公開

教育情報セキュリティポリシー（対策基準）及び教育情報セキュリティ実施手順は、公にすることにより小中学校の運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。