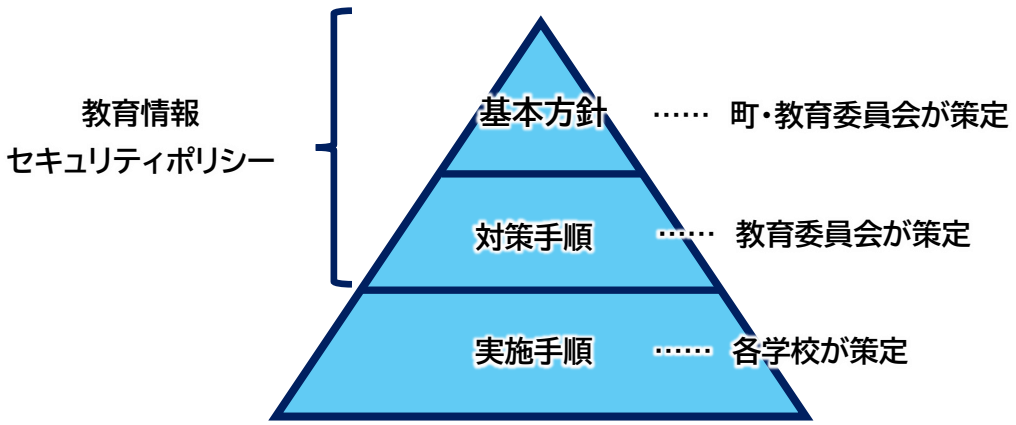
南幌町　教育情報セキュリティポリシー

令和７年１０月１日
第１版

はじめに

１．本教育情報セキュリティポリシーは、南幌町の小中学校における教育活動を支える情報資産の保護と、その安全かつ適切な活用を目的として策定された。現代の教育現場では、ＩＣＴ機器やデジタルデータの利用が不可欠であり、その運用には高いセキュリティ意識と責任が求められる。
２．これを怠り、情報が漏洩した場合、児童生徒や教職員等の個人情報が外部に流出し、学校や地域社会に大きな影響を及ぼす可能性がある。
３．本ポリシーでは、情報セキュリティを強化し、リスクを低減するための基本方針と具体的な対策基準、実施手順を明確に定めている（図表１）。すべての関係者がこれを遵守することで、安全で信頼性の高い教育環境を構築し、児童生徒が安心して学べる場を提供する。

【図表１】



例）
基本方針：学校の教育活動に関連するすべての情報資産を適切に管理する。
対策手順：ＵＳＢメモリを使用する場合には、情報管理責任者の承認を必要とする。
実施手順：ＵＳＢメモリを使用する場合には、利用者は管理台帳に氏名と使途を記入する。教頭は、台帳に押印することで承認する。

第１編　基本方針

１．本教育情報セキュリティポリシーは、教育活動を支える情報資産の保護とその適切な活用を通じて、安全で信頼性の高い学びの環境を構築することを目的とする。教育現場において、ＩＣＴ機器やデジタルデータの利用が拡大する中、児童生徒や教職員の個人情報や学習データを守ることは、地域社会全体の信頼を維持するうえで極めて重要である。

２．南幌町の小中学校では、以下の基本的な方針に基づき、情報セキュリティを確保する。

（１）　情報資産の保護

児童生徒、教職員等、関係者の個人情報や、学校の教育活動に関連するすべての情報資産を適切に管理し、不正アクセス、漏洩、改ざん、紛失などのリスクから保護する。

（２）　情報セキュリティ教育の推進

教職員等や児童生徒に対して、情報セキュリティの重要性を理解し、適切に対応できる知識と意識を育成するための教育を実施する。

（３）　運用の継続性の確保

教育活動や学校運営が継続的かつ安定的に行えるよう、情報セキュリティの維持・向上に努める。

（４）　法令および規範の遵守

情報セキュリティに関連する法令、規範、教育委員会の方針を遵守し、信頼性の高い運用体制を構築する。

（５）　継続的な見直しと改善

情報セキュリティ体制を定期的に評価し、変化する環境や技術に応じて適切な見直しと改善を行う。

第２編　対策基準

１．対象範囲及び用語説明

（１）　行政機関等の範囲

本対策基準が適用される行政機関等は、内部部局、南幌町教育委員会および南幌町立南幌小学校、南幌町立南幌中学校とする。

（２）　情報資産の範囲

本対策基準が対象とする情報資産は、以下のとおりとする。

①　教育ネットワーク、教育情報システム（校務・学習）、これらに関する設備、電磁的記録媒体

② 教育ネットワーク及び教育情報システムで取り扱う情報（これらを印刷した文書を含む）

（３） 用語説明

本対策基準における用語は、以下のとおりとする。

① 校務系情報

児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教員の個人情報など、学校が保有する情報資産のうち、それら情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報

② 校務外部接続系情報（公開系情報）

校務系情報のうち、保護者メールや学校ホームページ等インターネット接続を前提とした校務で利用される情報

③ 学習系情報

児童生徒のワークシート、作品など、学校が保有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ当該情報に教員及び児童生徒がアクセスすることが想定されている情報

④ 校務用端末

校務系情報にアクセス可能な端末

⑤ 学習者用端末

学習系情報にアクセス可能な端末で、児童生徒が利用する端末
児童生徒用の権限を付与されたアカウントで利用する、ＧＩＧＡスクール一人一台端末がこれに相当する

⑥ 指導者用端末

学習系情報にアクセス可能な端末で、教員のみが利用する端末
教員用の権限を付与されたアカウントで利用する、ＧＩＧＡスクール一人一台端末がこれに相当する

⑦ 教育情報システム

校務系システム、校務外部接続系システム及び学習系システムを合わせた総称

２．組織体制

（１） 最高教育情報セキュリティ責任者≪教育長≫

① 教育長を、最高教育情報セキュリティ責任者≪教育長≫とする。本町における全ての教育ネットワーク、教育情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権および責任を有する。

② 最高教育情報セキュリティ責任者≪教育長≫は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高教育情報セキュリティアドバイザー≪外部有識者≫として置き、その業務内容を定めるものとする。

③ 最高教育情報セキュリティ責任者≪教育長≫は、本町の全ての教育ネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

④ 最高教育情報セキュリティ責任者≪教育長≫は、本町の全ての教育ネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

⑤ 最高教育情報セキュリティ責任者≪教育長≫は、教育情報セキュリティ責任者≪課長≫、教育情報セキュリティ管理者≪校長≫、教育情報システム管理者≪課長≫及び教育情報システム担当者≪担当職員≫に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑥ 最高教育情報セキュリティ責任者≪教育長≫は、本町の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には必要かつ十分な措置を行う権限及び責任を有する。

⑦ 最高教育情報セキュリティ責任者≪教育長≫は、本町の共通的な教育ネットワーク、教育情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

⑧ 最高教育情報セキュリティ責任者≪教育長≫は、緊急時には、最高教育情報セキュリティアドバイザー≪外部有識者≫の助言を得て、回復のための対策を講じなければならない。

（２） 教育情報セキュリティ責任者≪課長≫

① 教育委員会事務局の情報セキュリティ担当部局の課長を教育情報セキュリティ責任者≪課長≫とする。

② 教育情報セキュリティ責任者≪課長≫は、本町の教育情報セキュリティ対策に関する統括的な権限及び責任を有する。

③ 教育情報セキュリティ責任者≪課長≫は、本町において所有している教育情報システムにおける開発、設定の変更、運用、見直し等を行う際の情報セキュリティに関する統括的な権限及び責任を有する。

④ 教育情報セキュリティ責任者≪課長≫は、本町において所有している教育情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び教職員等（教職員、非常勤教

職員及び臨時教職員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

（３） 教育情報セキュリティ管理者≪校長≫

① 校長を、教育情報セキュリティ管理者≪校長≫とする。

② 教育情報セキュリティ管理者≪校長≫は当該学校の情報セキュリティ対策に関する権限及び責任を有する。

③ 教育情報セキュリティ管理者≪校長≫は、当該学校において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、教育情報セキュリティ責任者≪課長≫、最高教育情報セキュリティ責任者≪教育長≫へ速やかに報告を行い、指示を仰がなければならない。

（４） 教育情報システム管理者≪課長≫

教育委員会の課長を、教育情報システムに関する教育情報システム管理者≪課長≫とする。

教育情報システム管理者≪課長≫は、所管する教育情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

教育情報システム管理者≪課長≫は、所管する教育情報システムにおける情報セキュリティに関する権限及び責任を有する。

教育情報システム管理者≪課長≫は、所管する教育情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（５） 教育情報システム担当者≪担当職員≫

教育委員会の担当職員を、教育情報システムに関する教育情報システム担当者≪担当職員≫とする。

教育情報システム担当者≪担当職員≫は、教育情報システム管理者≪課長≫の指示等に従い、教育情報システムの開発、設定の変更、運用、更新等の作業を行う。

（６） 教育情報セキュリティ委員会

① 本町の情報セキュリティ対策を統一的に行うため、最高教育情報セキュリティ責任者≪教育長≫、教育情報セキュリティ責任者≪課長≫、教育情報セキュリティ管理者≪校長≫、最高教育情報セキュリティアドバイザー≪外部有識者≫、および最高教育情報セキュリティ責任者≪教育長≫が別途選任した者から構成される情報セキュリティ委員会を設置し、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

② 情報セキュリティ委員会は、毎年度、情報セキュリティ対策の改善計画を策定し、その実施状況を確認することが望ましい。

（７） 情報セキュリティに関する統一的な窓口の設置

① 最高教育情報セキュリティ責任者≪教育長≫は、情報セキュリティインシデントの統一的な窓口の機能を有する組織を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

② 最高教育情報セキュリティ責任者≪教育長≫による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供する。

③ 情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

④ 情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

（８） 教職員等

臨時的任用教職員、非常勤講師を含めた教職員全員を、教職員等と称する。

教職員等は学校が所管する情報資産を取り扱う立場にあり、教育情報セキュリティ管理者≪校長≫の指導の下、情報セキュリティを遵守しなければならない。

（９） 教育委員会事務局職員

① 教育ネットワークを利用して、学校が所管する情報にアクセスできる教育委員会事務局職員を指す。

② 教育委員会事務局職員は学校の情報資産にアクセスできる立場にあり、教育情報セキュリティ責任者≪課長≫の指導の下、情報セキュリティを遵守しなければならない。

３．情報資産の分類と管理方法【情報資産の分類】

本町における情報資産は、機密性、完全性及び可用性の３つの観点から影響度を評価し、次のとおり４段階の重要性分類を行い、必要に応じて取扱制限を行うものとする。

Ⅰ．セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。

Ⅱ．セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす。

Ⅲ．セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす。

Ⅳ．影響をほとんど及ぼさない。

情報資産の分類		情報資産の例示			
重要性分類	定義	校務系		学習系	公開系
Ⅰ	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。	・指導要録原本 ・教職員の人事情報 ・入学者選抜問題 ・教育情報システム仕様書			
Ⅱ	セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす。	○学籍関係 ・卒業証書授与台帳 ・転退学受付（整理）簿 ・転入学受付（整理）簿 ・就学児童・生徒異動報告書 ・休学・退学願等受付（整理）簿 ・教科用図書給付児童・生徒名簿 ・要・準要保護児童・生徒認定台帳 ・その他校内就学援助関係書類 ○成績関係 ・通知表 ・評定一覧表 ・進級・卒業認定資料 ・定期考査・テスト等の答案用紙 （児童・生徒が記入済のもの） ・定期考査素点表 ・成績に関する個票等 ○指導関係 ・事故報告書・記録簿 ・生徒指導・特別指導等記録簿 ・児童・生徒等の個人写真・集合写真 ・指導記録・指導カード （児童・生徒等理解カード） ・教育相談・面接の記録・カード等 ・個別の教育支援計画 （学校生活支援シート） ・個別指導計画 ・家庭訪問記録・個別面談記録 ・教務手帳 ・週ごとの指導計画 （個人情報が含まれるもの） ○進路関係 ・調査書 ・推薦書 ・公立高校入学者選抜に係る成績一覧表 ・入学者選抜に関する表簿（願書等） ・私立高校入試に係る事前相談資料 ・卒業生進路先一覧等 ・進路希望調査 ・進路判定会議資料 ・進路指導記録簿	○児童・生徒に関する個人情報 （生活歴、心身の状況、財産状況等の情報、電話番号、メールアドレス、住所、生年月日、性別等の基本情報を含むもの） ○学校教職員に関する個人情報 （病歴、心身の状況、収入等の情報、電話番号、メールアドレス、住所、生年月日、性別等の基本情報を含むもの） ○健康関係 ・健康診断票 ・歯の検査表 ・心臓管理等医療情報 ・学校生活管理指導票 ・児童・生徒等健康調査票 ・児童・生徒の健康保険等被保険者証の写 ・健康診断に関する表簿 ・就学時健康診断票 ○教職員に割り当てた機密性の高い情報 ・情報システムログインID/PW管理台帳 ・情報端末ログインID/PW管理台帳 ○その他 ・給食関係書類・寄宿関係資料 ○名簿等 ・児童生徒名簿 ・保護者緊急連絡網 ・児童生徒の住所録 ・PTA会員名簿 ・職員緊急連絡網・職員住所録 ・委員会名簿 ・PTA役員連絡網 ○各種帳票ファイル ・指導要録作成システム等、データの入っていない帳票	○児童生徒の学習系情報 ・学習システムログインID/PW管理台帳 ・学習用端末ID/PW管理台帳	
Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす。	○児童生徒の氏名 ・出席簿 ・名列表 ・座席表 ・児童生徒委員会名簿	○学校運営関係 ・卒業アルバム ・学校行事等の児童・生徒の写真	○学校運営関係 ・授業用教材 ・教材研究資料 ・生徒用配布プリント ○児童生徒の学習系情報 ・児童生徒の学習記録 （確認テスト、ワークシート、レポート、作品等） ・学習活動の記録（動画・写真等）	
Ⅳ	影響をほとんど及ぼさない。				○学校運営関係 ・学校・学園要覧 ・学校紹介パンフレット ・使用教科書一覧 ・教育課程編成表 ・学校設定科目の届け出 ・特色紹介冊子原稿 ・学校徴収金会計簿 （学年費、教育振興費等） ・学校行事実施計画 （避難訓練・体育祭実施計画等） ・保護者等への配布文書文例 ・各種届雛形・校務分掌表 ・ＰＴＡ資料 ・学園・学校・学年・学級だより ・学校・学園ホームページ掲載情報 ・学校行事のしおり ○学校活動の記録 ※　保護者の承諾がある場合、以下は公開可能 ・学校行事等の児童・生徒の写真 ・学習活動の記録（動画・写真・作品等）

４．情報資産の分類と管理方法【情報資産の管理】

（１） 管理責任

① 最高教育情報セキュリティ責任者≪教育長≫は、教育情報システムとその運用管理を定めた学校教育情報セキュリティ対策基準を策定しなければならない。

② 教育情報セキュリティ管理者≪校長≫は、自校の所管する情報資産について管理責任を有する。

③　教育情報セキュリティ管理者≪校長≫は、教職員等の情報資産の取り扱いに際し、台帳及び実施手順に基づいた運用管理を指導しなければならない。

④　教職員等は、台帳及び実施手順に基づき、適切に情報資産を取り扱わなければならない。

（２）情報資産の取扱い

①　情報資産の分類の表示

教職員等は、情報資産について、その分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

②　情報の作成

（ア）　教職員等は、業務上必要のない情報を作成してはならない。

（イ）　情報を作成する教職員等は、情報の作成時に、前述Ⅰ～Ⅳの情報分類に基づき、当該情報の分類を定め、分類に準拠した取扱いを行わなければならない。

（ウ）　情報を作成する教職員等は、作成途上の情報についても、取扱いを許可されていない者の閲覧や紛失・流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

③　情報資産の入手

（ア）　本町教職員等が作成した情報資産を入手した教職員等は、入手元の情報資産の分類に基づき、当該情報の分類を定め、分類に準拠した取扱いを行わなければならない。

（イ）　本町教職員以外の者が作成した情報資産を入手した教職員等は、前述Ⅰ～Ⅳの分類に基づき、当該情報の分類を定め、分類に準拠した取扱いを行わなければならない。

（ウ）　情報資産を入手した教職員等は、その情報資産の分類が不明な場合、教育情報セキュリティ管理者≪校長≫に判断を仰がなければならない。

④　情報資産の利用

（ア）　情報資産を利用する教職員等は、業務以外の目的に情報資産を利用してはならない。

（イ）　情報資産を利用する教職員等は、情報資産の分類に応じ、適切な取り扱いをしなければならない。

（３）情報資産の保管

①　教育情報セキュリティ管理者≪校長≫又は教育情報システム管理者≪課長≫の措置事項

（ア） 教育情報セキュリティ管理者≪校長≫は、情報資産の保管先を定め、教職員等に周知しなければならない。

② 教職員等の遵守事項

（ア） 教職員等は、教育情報セキュリティ管理者≪校長≫が指定した保管先にのみ情報資産を保管しなければならない。

（イ） 教職員等は、重要性分類Ⅱ以上の情報資産を外部持ち出しする場合は、限定されたアクセスの措置設定（アクセス制限や暗号化）を行い、教育情報セキュリティ管理者≪校長≫の個別許可を得なければならない。なお、外部持ち出しツールに限定されたアクセスの措置決定（アクセス制限や暗号化）機能を有する場合には、有効にしなければならない。

（４） 情報資産の外部持ち出し

① 分類に応じた情報資産の外部持ち出し制限

（ア） 教職員等は、重要性分類Ⅱ以上の情報資産を外部持ち出しする場合は、限定されたアクセスの措置設定（アクセス制限や暗号化）を行い、教育情報セキュリティ管理者≪校長≫の個別許可を得なければならない。なお、外部持ち出しツールに限定されたアクセスの措置設定（アクセス制限や暗号化）機能を有する場合には、有効にしなければならない。

（イ） 重要性分類Ⅲの情報資産については、教職員等の外部持ち出しについて、教育情報セキュリティ管理者≪校長≫の判断で包括的許可を可とする。なお、外部持ち出しツールに限定されたアクセスの措置設定（アクセス制限や暗号化）機能を有する場合には、有効にしなければならない。

② 電子メール、外部ストレージサービスによる情報の送信

情報資産が組織内部（組織が利用するサーバやクラウドサービス等）から組織外部（家庭や地域、事業者等）に電子メール等により外部送信される場合は、情報資産分類に応じ以下を実施しなければならない。

（ア） 電子メール、外部ストレージサービスにより重要性分類Ⅲ以上の情報を外部送信する者は、限定されたアクセスの措置設定（アクセス制限や暗号化）を行わなければならない。

（イ） 利用する電子メール、外部ストレージサービスは教育委員会又は学校から提供される公式サービスのみを利用し、私的に契約したサービスを利用してはならない。

③　外部電磁的記録媒体を用いた情報の外部持ち出し

ＵＳＢメモリ等の物理的な媒体による情報の外部持ち出しでは、紛失・盗難リスクを伴うことから以下を遵守しなければならない。

（ア）　管理された外部電磁的記録媒体以外の使用禁止

教育委員会又は学校から支給された公的な媒体のみを利用することが望ましい。

（イ）　外部電磁的記録媒体の暗号化の徹底

暗号化機能付きの媒体を利用し、暗号化機能を活かすことが望ましい。

④　情報資産の公表

（ア）　教育情報セキュリティ管理者≪校長≫は、公開する情報が正しい内容であることを事前に確認し、誤公開を防がなければならない。

（イ）　教育情報セキュリティ管理者≪校長≫は、住民に公開する情報資産について、改ざんや消去されないように定期的に確認しなければならない。

（５）情報資産の廃棄

①　情報資産を廃棄する教職員は、重要性分類Ⅲ以上の情報が記載された紙媒体の書類を廃棄する場合には、内容が復元できないように細断、熔解又はこれに準ずる方法にて廃棄しなければならない。

②　情報を記録している電磁的記録媒体を利用しなくなった場合、情報を復元できないように処置したうえで廃棄しなければならない。

５．物理的セキュリティ【サーバ等の管理】

（１）サーバの冗長化

①　教育情報システム管理者≪課長≫は、校務系サーバその他の校務系情報を格納しているサーバを冗長化し、同一データを保持することが望ましい。

②　教育情報システム管理者≪課長≫は、学習系サーバその他の学習系情報を格納しているサーバのハードディスクを冗長化することが望ましい。

（２）機器の廃棄等

教育情報システム管理者≪課長≫は、機器を廃棄又はリース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

６．物理的セキュリティ【教職員等の利用する端末や電磁的記録媒体等の管理】

（１） 教育情報システム管理者≪課長≫は、不正アクセス防止のため、ログイン時のＩＤパスワードによる認証、加えて多要素認証の実施等、使用する目的に応じた適切な物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

（２） 教育情報システム管理者≪課長≫は、校務系システム、教育情報システムへアクセスする端末へのログインパスワードの入力を必要とするように設定しなければならない。

（３） 教育情報システムの管理者は、特に強固なアクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産を取り扱う端末に対し、当該データ暗号化等の措置により、不正アクセスや教員の不注意等による情報流出への対策を講じなければならない。

（４） 教育情報システム管理者≪課長≫は、パソコンやモバイル端末におけるマルウェア感染の脅威に対し、ウイルス対策ソフトの導入等の対策を講じなければならない。なお、ＯＳによっては標準的にウイルス対策ソフトを備えている製品、ＯＳとしてウイルス感染のリスクが低い仕組みとなっている製品などもあるため、実際に運用する端末において適切な対策を講じること。強固なアクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産を取り扱う端末に対し、当該端末の状況及び通信内容を監視し、異常、あるいは不審な挙動を検知する仕組み（ふるまい検知）等の活用を検討し、適切な対策を講じること。

（５） 教育情報システム管理者≪課長≫は、インターネットへ接続をする場合、教職員等のパソコン、モバイル端末に対して不適切なウェブページの閲覧を防止するウェブフィルタリング等の対策を講じなければならない。

７．物理的セキュリティ【学習者用端末のセキュリティ対策】

（１） 不適切なウェブページの閲覧防止

児童生徒が端末を利用する際に不適切なウェブページの閲覧を防止する対策を講じなければならない。

＜対策例＞

①フィルタリングソフト

②検索エンジンのセーフサーチ

③セーフブラウジング

（２） マルウェア感染対策

学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

８．物理的セキュリティ【ＰＣ教室等における学習者用端末や電磁的記録媒体の管理】

（１） 教育情報システム管理者≪課長≫は、パソコン及び電磁的記録媒体について、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

（２） 教育情報システム管理者≪課長≫は、情報システムへのアクセスにおけるログインパスワードの入力等による認証を設定しなければならない。

９．人的セキュリティ【教育情報セキュリティ管理者≪校長≫の措置事項】

（１） 教職員等の情報セキュリティ意識醸成

① 教育情報セキュリティ管理者≪校長≫は、教職員等に対して、日ごろから情報セキュリティに関する話題を積極的に提供し、情報セキュリティ研修を受講させるなど、積極的にセキュリティ認識の向上を図らなければならない。

② 教育情報セキュリティ管理者≪校長≫は、校内でセキュリティ事故につながりかねないヒヤリ・ハット事案を抑止するために、教職員等が事案を発見した際に、ただちに対処し、すみやかに報告が上がるよう、教職員等に対する情報セキュリティ意識の醸成と風通しのよい関係性維持に努めなければならない。

③ 情報セキュリティポリシー等の閲覧容易性確保

教育情報セキュリティ管理者≪校長≫は、教職員等が常に教育情報セキュリティポリシー及び実施手順を閲覧・確認できるように配慮しなければならない。

（２） 教職員等への情報セキュリティポリシー等の遵守指導

① 教育情報セキュリティ管理者≪校長≫は、新規採用教職員等及び他自治体から本町に新規赴任した教職員等、及び非常勤及び臨時の教職員に対し、教育情報セキュリティポリシー等遵守すべき内容を理解・浸透するように指導を行わなければならない。

（３） インターネット接続及び電子メール利用の制限

① 教育情報セキュリティ管理者≪校長≫は、教職員等に業務端末による作業を行わせる場合において、業務以外でのインターネット接続及び電子メールの利用をしないよう教職員等に指導しなければならない。

なおウェブフィルタリングの設定について、教職員等から相談があった場

合は、教育情報セキュリティ管理者≪校長≫に上申して、判断を仰がなければならない。

② 教育情報セキュリティ管理者≪校長≫は、パソコンやモバイル端末の機能は、教職員等の業務内容に応じて、不必要な機能については制限することが適切である。

（４） 自己点検の実施

① 教育情報セキュリティ管理者≪校長≫は、年１回、学校の自己点検を行わなければならない。

② 教育情報セキュリティ管理者≪校長≫は、自己点検の結果を情報セキュリティ委員会に報告しなければならない。

１０． 人的セキュリティ【教職員等の遵守事項】

教職員等は、教育情報セキュリティ管理者≪校長≫の指導の下、以下の規定を遵守しなければならない。

（１） 教育情報セキュリティポリシー等の遵守

教職員等は、教育情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに教育情報セキュリティ管理者≪校長≫に相談し、指示を仰がなければならない。

（２） 支給端末の取扱い

① 教職員等は、業務目的以外で支給端末を使用してはならない。

② 教職員等は、外部のソフトウェアを無断で支給端末にインストールしてはならない。業務上必要な場合には、事前に教育情報セキュリティ管理者≪校長≫の許可を得ること。

（３） ＩＤの取扱い

教職員等は、自己の管理するＩＤに関し、次の事項を遵守しなければならない。

① 自己が利用しているＩＤに関し、他人に利用させてはならない。

② 共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

（４） パスワードの取扱い

教職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

① パスワードは、他者に知られないように管理しなくてはならない。

② パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

③　パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

④　パスワードが流出したおそれがある場合には、教育情報セキュリティ管理者≪校長≫に速やかに報告し、パスワードを速やかに変更しなくてはならない。

⑤　仮のパスワード（初期パスワードを含む）は、最初のログイン時点で変更しなければならない。

⑥　教職員間でパスワードを共有してはならない。（ただし、共有ＩＤに対するパスワードは除く）

（５）クラウドサービス、ソーシャルメディアサービス利用制限

①　重要性分類Ⅱ以上の情報資産を、インターネットを通信経路としたパブリッククラウドサービスで取り扱ってはならない。なお、強固なアクセス制御になる対策を講じたシステム構成の場合は、その限りでない。

②　ソーシャルメディアサービスを利用して、業務上知りえた情報を公開してはならない。

（６）不正プログラム対策に関する教職員等の遵守事項

教職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①　パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
ＯＳ及びコンピュータウイルス対策ソフトウェアが常に最新の状態に保てるようにしなければならない。自動更新される設定の場合は、自動更新設定を変えてはならない。

②　差出人が不明又は不自然に添付されたファイルを受信した場合には、速やかに削除しなければならない。

③　最高教育情報セキュリティ責任者≪教育長≫が提供するウイルス情報を、常に確認しなければならない。

④　コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、速やかに教育情報セキュリティ管理者≪校長≫に報告し、指示を仰がなければならない。また、以下の対応を行わなければならない。

（ア）　パソコン等の端末の場合
有線ＬＡＮにつながる業務端末（校務用端末等）の場合は、ＬＡＮケーブルの即時取り外しを行わなければならない。

（イ）　モバイル端末の場合
無線ＬＡＮにつながる業務端末（指導者用端末及び学習者用端末）の

場合は、直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

（ウ） 指示があるまでは、端末の電源は切らずに保持しなければならない。

（７） 機器構成の変更の制限

① 教職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、最高教育情報セキュリティ責任者≪教育長≫及び教育情報システム管理者≪課長≫の許可を得なければならない。

（８） 児童生徒への指導事項

教職員等は、児童生徒に学習者用端末を利用させるにあたり、以下の事項について指導を行わなければならない。

① 学習用途の利用限定

学習者用端末及び学習系クラウドサービスは学習目的で利用すること。

② 利用者認証情報の秘匿管理

ＩＤ及びパスワードは他の人に知られないようにすること。

③ 学習系情報は学習系クラウドに保管

端末で生成した情報の保存先を学習系クラウドに指定できる機能がある場合には、この機能を利用して原則学習系クラウドに保管し、学習者用端末にローカル保存は必要最小限とすること。

④ コミュニケーションツールの利用制限

学校から許可されたコミュニケーションツール（ＳＮＳ，チャット等）のみを利用すること。

⑤ ウイルス感染が疑われる場合の報告

学習者用端末が動かない、勝手に操作される、いつもと異なる画面や警告が表示されるなどの症状が出た場合、すぐに担任教師に報告すること。

⑥ 端末の安全な取り扱い

学習者用端末は大事に取り扱い、盗難・紛失・破損等に注意すること。

（９） 異動・退職時等の遵守事項

教職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産（紙情報、データの格納された端末、外部記録媒体等）を返却しなければならない。また、その後も業務上知りえた情報を漏らしてはならない。

１１． 人的セキュリティ【教育委員会事務局職員の遵守事項】

教育委員会事務局職員は、教育情報セキュリティ責任者≪課長≫の指導の下、以下の規定を遵守しなければならない。

（１） 教育情報セキュリティポリシー等の遵守

（２） 業務以外の目的での使用の禁止

（３） 校務用端末による外部における情報処理作業の禁止

（４） 重要性分類Ⅱ以上の情報資産について校務用端末以外のパソコン、モバイル端末及び電磁的記録媒体等によるアクセスの禁止

（５） 知りえた情報の秘匿

（６） 業務を離れる場合の遵守事項

異動、退職等により業務を離れる場合には、利用していた情報資産をすべて返却する。また、その後も知り得た情報を漏らさない。

１２． 人的セキュリティ【研修・訓練】

（１） 情報セキュリティに関する研修・訓練

最高教育情報セキュリティ責任者≪教育長≫は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

（２） 研修計画の策定及び実施

① 最高教育情報セキュリティ責任者≪教育長≫は、教職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、情報セキュリティ委員会の承認を得なければならない。

② 研修計画において、教職員等は、毎年度最低１回は情報セキュリティ研修を受講できるようにすることが望ましい。

③ 新規採用の教職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

④ 研修は、最高教育情報セキュリティ責任者≪教育長≫、教育情報セキュリティ管理者≪校長≫、教育情報システム管理者≪課長≫、教育情報システム担当者≪担当職員≫及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

⑤ 最高教育情報セキュリティ責任者≪教育長≫は、毎年度１回、情報セキュリティ委員会に対して、教職員等の情報セキュリティ研修の実施状況について報告しなければならない。

（３） 研修・訓練への参加

全ての教職員等は、定められた研修・訓練に参加しなければならない。

１３． 人的セキュリティ【情報セキュリティインシデントの連絡体制の整備】

（１） 学校内からのセキュリティインシデントの報告

① 教職員等は、情報セキュリティインシデントを認知した場合、速やかに教育情報セキュリティ管理者≪校長≫に報告しなければならない。

② 報告を受けた教育情報セキュリティ管理者≪校長≫は、速やかに最高教育情報セキュリティ責任者≪教育長≫、教育情報システム管理者≪課長≫及び情報セキュリティに関する統一的な窓口に報告しなければならない。

（２） 教職員等の報告義務

① 教職員等は、教育情報セキュリティポリシーに対する違反行為を発見した場合、直ちに教育情報セキュリティ管理者≪校長≫へ報告しなければならない。

② 違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると最高教育情報セキュリティ責任者≪教育長≫が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

（３） 情報セキュリティインシデントの原因の究明・記録、再発防止等

① 最高教育情報セキュリティ責任者≪教育長≫は、情報セキュリティインシデントについて、教育情報セキュリティ管理者≪校長≫、教育情報システム管理者≪課長≫及び情報セキュリティに関する統一的な窓口と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、最高教育情報セキュリティ責任者≪教育長≫に報告しなければならない。

② 最高教育情報セキュリティ責任者≪教育長≫は、教育情報セキュリティ責任者≪課長≫から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

（４） 支給端末の運用・連絡体制の整備

学校内外での支給端末の運用ルールを制定し、インシデント発生時の連絡先対応方法を各学校にて整理し、実施手順に反映しなければならない。

１４． 技術的セキュリティ【コンピュータ及びネットワークの設定管理】

（１） バックアップの実施

最高教育情報セキュリティ責任者≪教育長≫及び教育情報システム管理者≪課長≫は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、次の①及び②に基づきバックアップを実施するものとする。

① 校務系情報及び校務外部接続系情報については、必要に応じて定期的にバックアップを実施しなければならない。

② 学習系情報については、必要に応じて定期的にバックアップを実施することが望ましい。

１５． 運用【職員等のＩＤ及びパスワードの管理】

（１） 利用者ＩＤの取扱い

① 最高教育情報セキュリティ責任者≪教育長≫及び教育情報システム管理者≪課長≫は、利用者の登録、変更、抹消等の情報管理、教職員等の移動、出向、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

② 最高教育情報セキュリティ責任者≪教育長≫及び教育情報システム管理者≪課長≫は、利用されていないＩＤが放置されないよう、人事管理部門と連携し、点検しなければならない。

（２） パスワードに関する情報の管理

① 最高教育情報セキュリティ責任者≪教育長≫又は教育情報システム管理者≪課長≫は、教職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

１６． 運用【児童生徒におけるＩＤおよびパスワード等の管理】

（１） ＩＤ登録・変更・削除

① 入学／転入時のＩＤ登録処理

ＩＤについてはシンプル・ユニーク（唯一無二）・パーマネント／パーシスタント（永続的な識別）な構成要素になっていることや、児童生徒の発達段階に応じた複雑性を上げたパスワードポリシーによりセキュリティ強度を上げていくなど適切な措置を講じなければならない。

② 転出／卒業／退学時のＩＤ削除処理

ユニークなＩＤは個人を識別できる可能性があるため、個人情報保護の観点から、サービス提供機関を超えて個人を特定する情報を保持しないようにする必要がある。

転出や卒業／退学時に学習用ツールのサービス利用期間が終了する場合は、あらかじめ児童生徒本人によるデータ移行をサービス利用期間内に実施し、ＩＤの利用停止後、最終的にはＩＤ及び関連するデータの完全削除を行うこと。

ただし、本人同意や個人情報保護条例に従った適切な管理の下、一部のデータを活用することは可能である。

（２） 学習用ツールへのシングルサインオン

学習履歴を活用したり、個人の成果物を保存するアプリケーションが増えてくると、サービス利用時に都度ＩＤ／パスワード等の認証情報を入力したり、サービス毎のアカウント情報管理が非常に煩雑になるため、一度の認証により一

定時間は各種サービスにアクセスが行えるシングルサインオンの導入を行うことが望ましい。

１７．　運用【教育情報セキュリティポリシーの遵守状況の確認・管理】

（１）遵守状況の確認及び対処

①　教育情報セキュリティ責任者≪課長≫及び教育情報セキュリティ管理者≪校長≫は、教育情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに最高教育情報セキュリティ責任者≪教育長≫に報告しなければならない。

②　最高教育情報セキュリティ責任者≪教育長≫は、発生した問題について、適切かつ速やかに対処しなければならない。

③　最高教育情報セキュリティ責任者≪教育長≫及び教育情報システム管理者≪課長≫は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

（２）パソコン、モバイル端末および電磁的記録媒体等の利用状況調査

最高教育情報セキュリティ責任者≪教育長≫が指名した者は、不正アクセス、不正プログラム等の調査のために、教職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録の利用状況を調査することができる。

（３）教職員等による不正アクセスの管理

最高情報セキュリティ責任者及び教育情報システム管理者≪課長≫は、教職員等による不正アクセスを発見した場合は、当該職員等が所属する学校等の教育情報セキュリティ管理者≪校長≫に通知し、適切な対処を求めなければならない。

１８．　運用【侵害時の対応等】

（１）緊急時対応計画の作成

最高教育情報セキュリティ責任者≪教育長≫又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、セキュリティの侵害時には当該計画に従って適切に対処しなければならない。

（２）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

①　関係者の連絡先

②　発生した事案に係る報告すべき事項

③　発生した事案への対応措置

④　再発防止措置の策定

（３）業務継続計画との整合性確保

自然災害、大規模又は広範囲に及ぶ疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

（４）緊急時対応計画の見直し

最高教育情報セキュリティ責任者≪教育長≫又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

１９．　運用【法令等遵守】

（１）教職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令等を遵守し、これに従わなければならない。

①　地方公務員法（昭和 25 年 12 月 13 日法律第 261 号）

②　地方公務員特例法（昭和 24 年 1 月 12 日法律第 1 号）

③　著作権法（昭和 45 年法律第 48 号）

④　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）

⑤　個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）

⑥　行政手続における個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）

⑦　サイバーセキュリティ基本法（平成 26 年法律第 104 号）