十津川村教育委員会

教育情報セキュリティポリシー

令和６年２月１日

１．目的

この「教育情報セキュリティポリシー」は、十津川村のすべての小中学校が保有する情報資産の機密性、完全性及び可用性を確保ならびに維持するために必要な基本事項等を定めることを目的とする。

２．基本方針

「十津川村情報セキュリティポリシー」における基本方針に従う。なお、本ポリシーに未記載の事項については、原則として「教育情報セキュリティポリシーに関するガイドライン（文部科学省）」に準ずるものとする。

３．組織体制

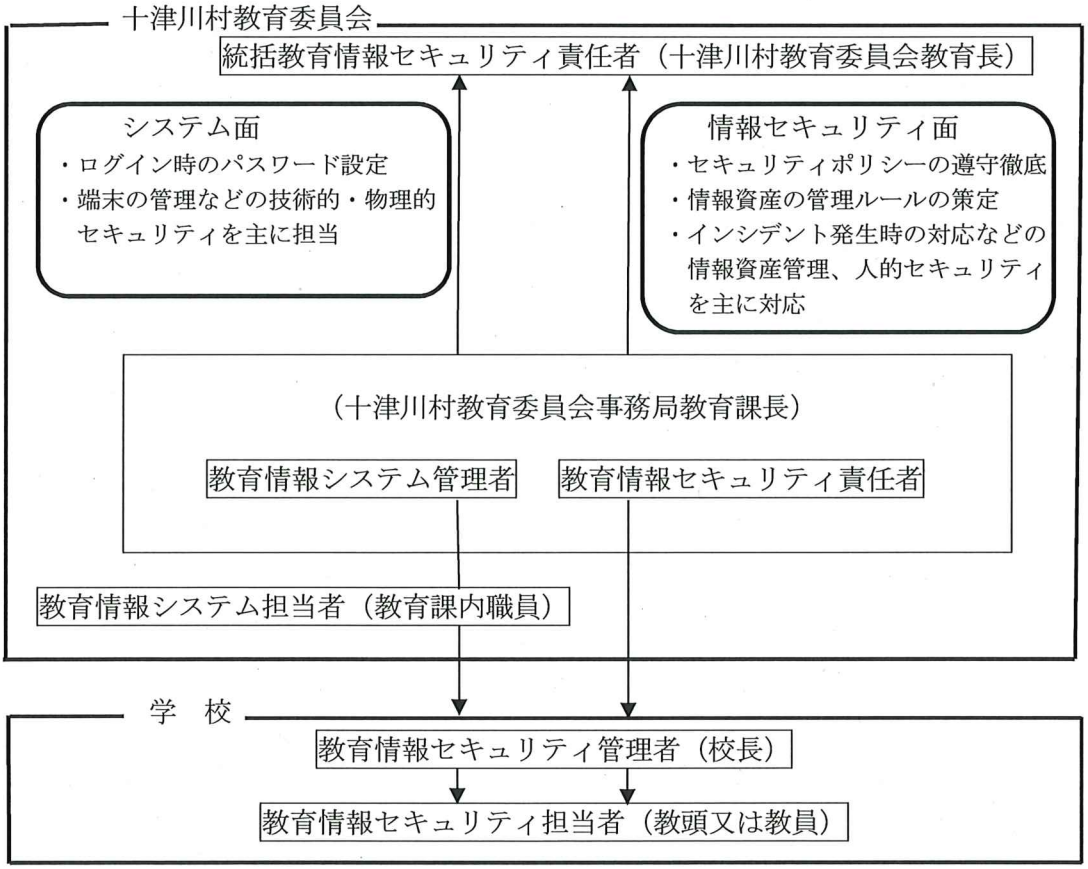
（1） 十津川村教育委員会は、設置する学校における教育情報セキュリティ全般を管理し、その統括教育情報セキュリティ責任者を十津川村教育委員会教育長（以下「教育長」という）とする。

（2） 教育情報セキュリティ責任者と教育情報システム管理者を、十津川村教育委員会事務局教育課長（以下「課長」という。）が兼ねる。

（3） 教育情報システム担当者を、十津川村教育委員会事務局教育課職員より選任する。

（4） 設置された学校においては、当該の校長を教育情報セキュリティ管理者とし、教育情報セキュリティ担当者を当該学校の教頭又は教員より選任する。

【十津川村教育委員会に関する情報セキュリティ推進組織体制図】



（解説）

・統括教育情報セキュリティ責任者【教育長】

統括教育情報セキュリティ責任者は、村内の全ての教育ネットワークや教育情報システムの開発、設定の変更、運用、見直し等の権限及び責任を有するほか、情報セキュリティ対策に関する権限及び責任を有する。また、情報セキュリティインシデント発生時等の緊急時には、統括教育情報セキュリティ責任者が中心となり被害の拡大防止、事態の回復のための対策実施、再発防止策の検討を行う必要がある。

・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責任者は、教育情報セキュリティ対策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】

教育情報システム管理者は、個々の教育情報に関する権限及び責任を有する。さらに、個々の教育情報システムの開発、設定の変更、運用、見直し等の権限及び責任を有するほか、所管する教育情報システムに対する情報セキュリティ対策に関する権限及び責任を負う。

・教育情報セキュリティ管理者【校長】

教育情報セキュリティ管理者は、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。

教育情報セキュリティ管理者は、システムの利用現場の担当者であり、学校において、情報資産に対するセキュリティ侵害又はセキュリティ侵害のおそれがある状況に直面する可能性が高い。そのため、このような場合を想定し、教育情報セキュリティ責任者及び統括教育情報セキュリティ責任者に対する報告義務を定める。

・教育情報システム担当者【教育課内職員】

教育情報システム担当者は、教育情報システム管理者の指示等に従う職員で、開発、設定等の変更、運用、見直し等の作業を行う。

・教育情報セキュリティ担当者【教頭又は教員】

教育情報セキュリティ担当者は、教育情報セキュリティ管理者の指示等に従い、教育情報セキュリティポリシーの遵守について全教職員への周知を行う責任を有する。

４．対策基準

（１） 情報資産の分類

① 学校が保有する校務系情報・校務外部接続系情報・学習系情報全ての情報資産を、把握すること。なお、情報資産の分類や情報資産の取扱い等の注意事項については、別添の分類表（教育情報セキュリティポリシーに関するガイドラインより）を参考にすること。

（解説）

・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

・校務外部接続系情報

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

・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

② 情報資産の重要度による仕分け整理を行うこと。その際に、情報を漏えいさせない（機密性を確保）、情報を改ざんさせない（完全性を確保）、情報がいつでも扱える状態を保つ（可用性を確保）の３つの観点から影響度を評価し分類すること。

（解説）

・機密性　　情報資産の利用を許可された者だけが、利用できる状態を確保すること。
・完全性　　情報資産が漏えい・破壊・改ざん又は消去されない状態を確保すること。
・可用性　　情報資産の利用を許可された者が、必要なときに中断されることなく、情報資産の利用ができる状態を確保すること。

（２） 情報資産の管理

① 管理責任

（ア） 教育情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

（イ） 情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

② 情報資産の分類の表示

教職員は、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。

※ 情報資産の分類の表示先

・ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）

・紙媒体による情報ファイル等のラベル表示

③ 情報の作成

(ア) 教職員は、業務上必要のない情報を作成してはならない。

(イ) 情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ウ) 情報を作成する者は、作成途上の情報についても、紛失や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。

④ 情報資産の入手

(ア) 学校内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

(イ) 学校外の者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ウ) 情報資産を入手した者は、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に判断を仰がなければならない。

⑤ 情報資産の利用

(ア) 情報資産を利用する者は、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者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

(ウ) 情報資産を利用する者は、保存されているクラウド領域に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従ってその領域を取り扱わなければならない。

⑥ 情報資産の保管

(ア) 教育情報セキュリティ管理者又は教育情報システム管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

(イ) 教育情報セキュリティ管理者又は教育情報システム管理者は、情報資産をデジタルデータとして保管する場合は、教育委員会が管理するサーバまたはクラウドサービスを利用し保管しなければならない。また、そのクラウドサービスの機能として自然災害対策がなされていることを確認しなければならない。

(ウ) 教職員は、原則として情報資産の保管のために電磁的記録媒体を利用してはならない。ただし、重要性分類Ⅲ以上の情報を記録したDVD等を保管する必要がある場合は、耐火、耐震等を講じた施錠可能な場所に保管しなければならない。

⑦ 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) 電子メール等により重要性分類Ⅲ以上（機密性2A以上）の情報を外部送信する必要がある場合は、その権限を有する者のみ（学校においては管理職）が行わなければならない。

(イ) 教育情報セキュリティ管理者及び教育情報システム管理者は、電子メール等による外部送信の安全性を高めるため、添付される情報資産を監視する等、出口対策を実施することが望ましい。

⑧ 情報資産の運搬 ≪原則禁止≫

(ア) 車両等により重要性分類Ⅲ以上（機密性2A以上）の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

(イ) 重要性分類Ⅲ以上（機密性 2A 以上）の情報資産を運搬する者は、教育情報セキュリティ管理者に許可を得なければならない。

⑨ 情報資産の提供・公表

(ア) 重要性分類Ⅲ以上（機密性 2A 以上）の情報資産を外部に提供する者は、限定されたアクセスの措置設定（アクセス制限や暗号化、パスワード設定等）を行わなければならない。

(イ) 重要性分類Ⅲ以上（機密性 2A 以上）の情報資産を外部に提供する者は、教育情報セキュリティ管理者に許可を得なければならない。

(ウ) 教育情報セキュリティ管理者及び教育情報システム管理者は、保護者等に公開する情報資産について、完全性を確保しなければならない。

⑩ 情報資産の廃棄

(ア) 重要性分類Ⅲ以上（機密性 2A 以上）の情報資産を廃棄する者は、情報を復元できないように処置しなければならない。

(イ) 情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

(ウ) 情報資産の廃棄を行う者は、教育情報セキュリティ管理者の許可を得なければならない。

(3) 技術的セキュリティ

① パソコン及びモバイル端末の管理

(ア) 電子メールの利用制限

・ 教職員は、自動転送機能を用いて、電子メールを転送してはならない。
・ 教職員は、業務上必要のない送信先に電子メールを送信してはならない。
・ 教職員は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
・ 教職員は、重要な電子メールを誤送信した場合、教育情報セキュリティ管理者に報告しなければならない。
・ 教職員は、ウェブで利用できるフリーメールサービス等を統括教育情報セキュリティ責任者の許可無しに使用してはならない。

(イ) 無許可ソフトウェアの導入等の禁止

・ 教職員は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。
・ 教職員は、業務上の必要がある場合は、統括教育情報セキュリティ責任者及び教育情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、教育情報セキュリティ管理者又は教育情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。
・ 教職員は、不正にコピーしたソフトウェアを利用してはならない。

(ウ) 機器構成の変更の制限

教職員は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

(エ) 業務以外の目的でのウェブ閲覧の禁止

・ 教職員は、業務以外の目的でウェブを閲覧してはならない。
・ 統括教育情報セキュリティ責任者は、教職員のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、教育情報セキュリティ管理者に通知し適切な措置を求めなければならない。

② 不正プログラム・不正アクセス対策

(ア) 教職員の遵守事項

・ 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は、速やかに削除しなければならない。
・ 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、即座にパソコン等の利用中止し、被害の拡大を防がなければならない。

(イ) 教職員による不正アクセス

統括教育情報セキュリティ責任者及び教育情報セキュリティ管理者は、教職員によ

る不正アクセスを発見した場合は、当該教職員が所属する学校の教育情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

（ウ） 教職員の報告義務

・ 教職員は、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、直ちに統括教育情報セキュリティ責任者及び教育情報セキュリティ管理者に報告を行わなければならない。

・ 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統括教育情報セキュリティ責任者が判断した場合は、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。

（4） 人的セキュリティ

① 教職員の遵守事項

（ア） 教育情報セキュリティポリシー等の遵守

教職員は、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に相談し、指示を仰がなければならない。

（イ） 業務以外の目的での使用の禁止

教職員は、業務以外の目的で情報資産の外部への持ち出し、教育情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

（ウ） ＩＤ及びパスワードの取扱い

・ 自己が利用しているＩＤは、他人に利用させてはならない。

・ 共有ＩＤを利用する場合は、共有ＩＤの利用者以外に利用させてはならない。

・ パスワードは、他人に知られないように管理しなければならない。

・ 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。

・ 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。

・ 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に速やかに報告し、パスワードを速やかに変更しなければならない。

・ 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。

・ サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。

・ 教職員間でパスワードを共有してはならない。

・ 共有ＩＤに対するパスワードは定期的に又はアクセス回数に基づいて変更しなければならない。

・ 取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の多要素認証を設定しなければならない。

（エ） モバイル端末等の持ち出し及び教育委員会・学校が構築・管理している環境（本ガイドラインが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境）の外部における情報処理作業の制限

・ 教職員は、学校外での利用が認められているモバイル端末を外部に持ち出す場合には、教育情報セキュリティ管理者の許可を得なければならない。

・ 教職員は、外部で情報処理業務を行う場合には、教育情報セキュリティ管理者の許可を得なければならない。

（オ） ＵＳＢなどの電磁的記録媒体等及び学校指定以外のパソコン・モバイル端末の利用について

・ 教職員は、ＵＳＢなどの電磁的記録媒体等及び学校指定以外のパソコン・モバイル端末を、校内ネットワークに接続してはならない。また、校内に持ち込んで業務に利用してはならない。

・ 教職員は、学校指定以外のパソコン、モバイル端末を用いて、外部で情報処理作業を行う必要がある場合には、教育情報セキュリティ管理者の許可を得た上で、安全管

理措置を遵守しなければならない。

(カ)　持ち出し及び持ち込みの記録

教育情報セキュリティ管理者は、支給端末の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

※　記録簿の記入項目例

（出）名前、日時、返却日予定日、持出物、用途、使用場所、管理者の確認印

（入）返却日、管理職の確認印

(キ)　パソコンやモバイル端末におけるセキュリティ設定変更の禁止

教職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を教育情報セキュリティ管理者の許可なく変更してはならない。

(ク)　机上の端末等の管理

教職員は、パソコン、モバイル端末及び情報が印刷された文書等について、第三者に使用されること又は校長の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや、文書等が容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

(ケ)　退職時等の遵守事項

教職員は、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を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

②　非常勤及び臨時の教職員への対応

(ア)　教育情報セキュリティポリシー等の遵守

教育情報セキュリティ管理者は、非常勤及び臨時の教職員に対し、採用時に教育情報セキュリティポリシー等のうち、非常勤及び臨時の教職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

(イ)　教育情報セキュリティポリシー等の遵守に対する同意

教育情報セキュリティ管理者は、非常勤及び臨時の教職員の採用の際、必要に応じ教育情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

(ウ)　インターネット接続及び電子メール使用等の制限

教育情報セキュリティ管理者は、非常勤及び臨時の教職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

③　情報セキュリティポリシー等の掲示

教育情報セキュリティ管理者は、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できるように掲示しなければならない。

④　外部委託事業者に対する説明

教育情報システム管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

⑤　情報セキュリティインシデントの対応について

(ア)　緊急時対応計画の整備

総括教育情報セキュリティ責任者は、情報セキュリティインシデント発生時に対応するための、緊急時対応計画を定めておき、セキュリティ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。

(イ)　学校内からの情報セキュリティインシデントの報告

・　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に報告しなければならない。

・　報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ管理者および教育情報システム管理者に報告しなければならない。

(ウ)　住民等外部からの情報セキュリティインシデントの報告

・　教職員等は、情報セキュリティインシデントについて、保護者や住民等外部から報告を受けた場合、教育情報セキュリティ管理者に報告しなければならない。

・　報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ管理者および教育情報システム管理者に報告しなければならない。

(エ)　情報セキュリティインシデント原因の究明・記録、再発防止等

統括教育情報セキュリティ管理者は、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及び教育情報システム管理者と連携し、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た上で、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。

5．クラウドサービスの利用

下記(1)、(2)に関する内容は、「教育情報セキュリティポリシーに関するガイドライン(文部科学省)」記載の詳細に従う。

(1)　クラウドサービスの利用における情報セキュリティ対策

①　利用者認証
②　アクセス制御
③　クラウドに保管するデータの暗号化
④　マルチテナント環境におけるテナント間の安全な管理
⑤　クラウドサービスを提供する情報システムに対する外部からの悪意のある脅威の侵入を想定した技術的セキュリティ対策
⑥　情報の通信経路のセキュリティ確保
⑦　クラウドサービスを提供する情報システムの物理的セキュリティ対策
⑧　クラウドサービスを提供する情報システムの運用管理
⑨　クラウドサービスを提供する情報システムのマルウェア対策
⑩　クラウド利用者側のセキュリティ確保
⑪　クラウド事業者従業員の人的セキュリティ対策
⑫　データの廃棄等について

(2)　パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項

①　守秘義務、目的外利用及び第三者への提供の禁止
②　準拠する法令、情報セキュリティポリシー等の確認
③　クラウド事業者の管理体制
④　クラウド事業者従業員への教育
⑤　情報セキュリティに関する役割の範囲、責任分界点
⑥　監査
⑦　情報インシデント管理及び対応フローの合意
⑧　クラウドサービスの提供水準及び品質保証
⑨　クラウド事業者の再委託先等の合意事項
⑩　その他留意事項

6．一人一台端末におけるセキュリティ

(1)　児童生徒への指導事項

①　モバイル端末を学校外へ持ち出す場合は、教員の許可を得ること。
②　データを端末内部に保存してはいけないこと。全てのデータ処理はクラウドサービス上にて行うこと。
③　モバイル端末等のソフトウェアに関するセキュリティ機能の設定を、教員の許可なく変更してはいけないこと。
④　自分のIDは、他人に利用させてはいけないこと。
⑤　パスワードを他人に知られないようにすること。
⑥　受信メールについて、送り主やタイトルで不審をいだいたメールは、クリックする前に教員に報告すること。

(2)　運用・連絡体制

一人一台端末の利活用について、児童生徒及び保護者へ学校側が規定する各種ガイドラインを正しく理解させるとともに、児童生徒の情報リテラシー教育を促す。また、インシデント発生時の報告に関して、その手順を周知徹底する。

（3） ID の登録・変更・削除

入学/転入学/進級/進学/転出/卒業等における ID 及び当該 ID に付随する個人情報の管理について、教育情報セキュリティ管理者は、教育情報システム管理者と連携して適切に処理をしなければならない。

7．教育情報セキュリティ実施状況の点検・確認

情報セキュリティを適切に確保するためには、情報セキュリティ対策の必要性と内容を全ての教職員等が十分に理解していることが必要不可欠である。また、情報セキュリティインシデントの多くは、教職員等の規定違反に起因している場合もある。さらに、情報セキュリティの向上は、利便性の向上とは、必ずしも相容れない場合もあり、教職員が業務を優先することが、情報セキュリティ対策の軽視につながることもある。このような状況を鑑み、情報セキュリティポリシーの遵守状況を点検・把握し、セキュリティ対策の状態や不備な部分を洗い出し改善を繰り返すこと、情報セキュリティへの脅威及び技術等の変化や点検・監査の結果等を踏まえ、教育情報セキュリティポリシー及び関係規定等を定期的に見直すこと、さらに、情報セキュリティ遵守のため、教職員全員の共通理解を徹底することが重要である。

8．情報セキュリティに関する主要な法令

教職員は、職務の遂行において使用する情報資産を保護するため、下記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。

- 地方公務員法（昭和 25 年法律第 261 号）
- 教育公務員特例法（昭和 24 年法律第 1 号）
- 著作権法（昭和 45 年法律第 48 号）
- 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）
- 個人情報の保護に関する法律（平成 15 年法律第 57 号）
- 行政手続における特定の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）
- 十津川村個人情報の保護に関する法律施行条例（令和５年条例第４号）