○野沢温泉村教育情報セキュリティポリシー

（野沢温泉村教育情報セキュリティー規程）

令和８年２月18日教委訓令第１号

目次

第１章　総則

（趣旨）

第１条　この規程は、野沢温泉村教育委員会及び野沢温泉村学校設置条例（昭和39年野沢温泉村条例第32号）に規定する小学校及び中学校（以下「学校」という。）における、ネットワーク及びシステムの設備、電磁的記録媒体等、又はそれらで取り扱う情報及び文書等（以下「情報資産」という。）の保護を目的に、情報セキュリティ対策について基本的な事項を定めるものである。

（定義）

第２条　この規程において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

⑴　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、教職員の個人情報など学校が保有する情報資産のうち、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をいう。

⑵　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、学校ホームページ等インターネット接続を前提として校務で利用される情報をいう。

⑶　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をいう。

⑷　校務用端末　校務系情報にアクセス可能な端末をいう。

⑸　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をいう。

⑹　指導者用端末　学習系情報にアクセス可能な端末で、教職員のみが利用可能な端末をいう。

⑺　校務系システム　学籍管理や教務、保健等の学校事務を行うため教職員が利用するシステムをいう。

⑻　学習系システム　授業の効果的な実施のために、教職員及び児童生徒が利用するシステムをいう。

⑼　教育ネットワーク　校務系及び学習系の端末やシステムを利用するための通信網及びその構成機器（ソフトウェア含む。）で構成された、情報処理を行う仕組みをいう。

⑽　教育系システム　校務系及び学習系のシステムやそれを利用するためのネットワーク等を合わせた総称をいう。

⑾　電磁的記録媒体　情報資産を扱うサーバ装置（クラウドサービスを除く。）、端末、デジタルカメラ等に内蔵される内蔵電磁的記録媒体と、ＵＳＢメモリ、外付けハードディスク等の外部電磁記録媒体をいう。

（位置づけ）

第３条　このセキュリティーポリシーは、野沢温泉村情報セキュリティポリシー基本方針及び対策基準（以下「村情報セキュリティポリシー」という。）に基づき、学校等における情報セキュリティ対策基準を定めたものである。

（対象範囲）

第４条　対象範囲は、野沢温泉村教育ネットワークを利用する教育委員会事務局、学校に属する全ての教職員及び外部受託者（以下「教職員等」という。）とする。

（対策基準の策定方針）

第５条　対策基準は、次に掲げる情報セキュリティ対策について、総合的かつ具体的に定めるものとする。

⑴　物理的セキュリティ対策　情報システム機器及びネットワーク機器等、ハードウェアの設置や保守・管理、配線や電源等の対策

⑵　人的セキュリティ対策　情報セキュリティに関する管理体制の整備、教職員の遵守事項及び研修の実施等の対策

⑶　技術的セキュリティ対策　情報システム及びネットワークに係る管理、アクセ

ス制御、不正プログラムや不正アクセス対策、システム調達管理等の対策

⑷　運用　不正利用等を防ぐための情報システムの監視に係る対策

⑸　外部サービスの利用　外部委託を行う際やクラウドサービス利用する際の、情報セキュリティ確保上必要な規定や対策

⑹　１人１台端末のセキュリティ対策　ＧＩＧＡスクール構想における１人１台端末の整備に伴い、学校内外で利用される学習者用端末の運用や連絡体制等の対策

⑺　評価及び見直し　監査及び自己点検の実施やその方法、評価に基づく規程の見直し等の対策

第２章　組織及び体制

（村情報セキュリティポリシーの適用）

第６条　組織及び体制については、村情報セキュリティポリシー第２章１に定めるもののほか必要な事項は、次条から第12条に定めるところによる。

（教育情報統括責任者の職務）

第７条　教育長を教育情報統括責任者（教育ＣＩＯ：Ｃｈｉｅｆ　ＩｎｆｏｒｍａｔｉｏｎＯｆｆｉｃｅｒ。以下「教育ＣＩＯ」という。）とし、教育委員会及び学校における情報化の推進と利活用、教育系システムに係る意思決定を行う権限と責任を有する。

（統括教育情報セキュリティ責任者の職務）

第８条　教育ＣＩＯは統括教育情報セキュリティ責任者を兼務し、村情報セキュリティポリシーに定めるＣＩＳＯ（最高情報セキュリティ責任者：Ｃｈｉｅｆ　ＩｎｆｏｒｍａｔｉｏｎＳｅｃｕｒｉｔｙＯｆｆｉｃｅｒ。以下「ＣＩＳＯ」という。）を補佐し、事故があるときは、教育系システムに係る事案に限りその職務を代理する。

２　統括教育情報セキュリティ責任者は、教育情報セキュリティ責任者をはじめ、全ての教職員等に対し情報セキュリティに関する教育、訓練、助言及び指示を行わなければならない。

（教育情報セキュリティ責任者）

第９条　教育次長を教育情報セキュリティ責任者とし、教育委員会及び学校における情報セキュリティ対策に関する事項を統括する。

２　教育情報セキュリティ責任者は、教育情報セキュリティ管理者及びその管理下にある教職員等に対し情報セキュリティに関する教育、訓練、助言及び指示を行わなければならない。

（学校情報統括責任者）

第10条　各学校の長を学校情報統括責任者（以下「学校ＣＩＯ」という。）とし、学校

内における情報マネジメント体制の整備や利活用に係る意思決定を行う権限と責任を有する。

（教育情報セキュリティ管理者）

第11条　学校ＣＩＯは教育情報セキュリティ管理者を兼務し、学校内における情報セキュリティ対策に関する事項を統括する。

２　教育情報セキュリティ管理者は、学校内において情報セキュリティ事案が発生した時、又はそのおそれがある時には、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へ速やかに報告を行い、指示を仰がなければならない。

（教育情報システム管理者）

第12条　こども支援係長を教育情報システム管理者とし、所管する教育系システムに関して次に掲げる職務を所掌する。

⑴　システムの開発、設定の変更、運用及び見直し等

⑵　情報セキュリティに関する適正な運用及び管理についての検討

⑶　教職員等に対するセキュリティ教育、訓練、助言及び指示

２　教育情報システム管理者は、前項に掲げる職務を遂行するに当たっては、村情報セキュリティポリシーに定める情報システム管理者（以下、「村情報システム管理者」という。）へ速やかに報告するとともに、必要な場合には指示を仰がなければならない。

第３章　情報資産の分類と管理

（情報資産の分類）

第13条　情報資産は、次に掲げる重要性分類に従って分類する。

⑴　重要性分類Ⅰ　機微な個人情報を含む校務系情報のなかで、特に機密性の高い情報で、学校外への流出や改ざんにより、教職員等又は児童生徒の生命、財産、プライバシー等に重大な支障を及ぼす情報。ただし、重要性分類Ⅰは、村対策基準における機密性３相当（かつ完全性２、可用性２相当を含み得る）として取り扱う。

⑵　重要性分類Ⅱ　機微な個人情報を含む校務系情報で、学校外への流出や改ざんにより、学校事務及び教育活動に重大な影響を及ぼす情報

⑶　重要性分類Ⅲ　学習中の段階にある学習系情報等個人情報が含まれる可能性のある情報で、学校外への流出や改ざんにより学校事務及び教育活動に軽微な影響を及ぼす情報

⑷　重要性分類Ⅳ　個人情報を含まない情報や公表を前提とした情報等、影響をほとんど及ぼさない情報

（情報資産の管理）

第14条　教職員等は、業務に必要のない情報を作成したり、業務以外の目的で情報資産を利用したりしてはならない。

２　情報資産は、前条に定める分類に応じ取扱い制限を定める。

３　前項に掲げる取扱い制限のほか、情報資産の管理について遵守すべき事項及びその方法については、教育情報セキュリティ管理者が実施手順において定めるものとする。

（管理責任）

第15条　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。

第４章　物理的セキュリティ対策

（管理区域の管理）

第16条　教育情報セキュリティ管理者は、ネットワークの基幹機器等や電磁的記録媒体その他情報機器の管理及び運用を行うための部屋等、情報資産の保護に際し重要な区域を明示しなければならない。

２　教育情報セキュリティ管理者は、前項の規定により明示した区域（以下、「管理区域」という。）については、その入退室を許可された者のみに制限しなければならない。

３　教育情報セキュリティ管理者は、児童生徒及び外部からの訪問者等が管理区域に立入る場合には、必要に応じて立入り区域を制限した上で、教職員等が付き添う等、安全確保上必要な措置を講じなければならない。

４　前項までの規定の他、管理区域の管理について遵守すべき事項及びその方法については、教育情報セキュリティ管理者が実施手順において定めるものとする。

（機器等の搬入及び搬出）

第17条　教育情報システム管理者は、搬入する機器等が既存の情報システム等に与える影響について、あらかじめ確認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及び教育情報システム管理者は、管理区域への機器等の搬入及び搬出については、教職員等を立ち会わせなければならない。

（通信回線の管理）

第18条　統括教育情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限とし、できる限り接続ポイントを減らすよう努めなければならない。

２　統括教育情報セキュリティ責任者は、通信回線を利用して重要性分類Ⅰ及びⅡの情報資産を取り扱う情報システムを使用する場合、適切な回線を選択するとともに、必要に応じて送受信される情報の暗号化等、必要な措置を講じなければならない。

（端末及び電磁的記録媒体の管理）

第19条　教職員等は、端末及び電磁的記録媒体の使用について、以下の事項を遵守しなければならない。ただし、教育情報セキュリティ管理者が必要と認める場合を除く。

２　校務用端末及び指導者用端末は、児童生徒の利用を原則禁止とする。

３　校務用端末は、業務外の利用及び校外への持ち出しを原則禁止とする。

４　校務用端末は、職員室で保管する等盗難等の防止に努めなければならない。また、事前に許可された以外の電磁的記録媒体を使用してはならない。

５　学習者用端末は、保管庫等による管理を行い盗難等の防止に努めなければならない。また、学習者用端末で教職員等及び児童生徒の私物である電磁的記録媒体を使用してはならない。

６　電磁的記録媒体を使用する場合、情報を保存する必要がなくなった時点で、記録した情報を速やかに削除しなければならない。

７　教育情報セキュリティ管理者は、校務情報等の重要な情報資産にアクセスする端末について、ウイルス対策など適切な情報セキュリティ対策を講じなければならない。

８　教育情報セキュリティ管理者は、第１項に定める例外措置について、実施手順において明示しなければならない。

第５章　人的セキュリティ対策

（教職員等の遵守事項）

第20条　教職員等は、本教育情報セキュリティーポリシー及び各校の実施手順を遵守しなければならない。この場合において、情報セキュリティ対策について不明確な点や遵守することが困難な点等がある場合には、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。

２　教職員等は、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。

３　教職員等は、モバイル端末を含む学校設置の端末、電磁的記録媒体、情報資産及びソフトウェア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。

４　教職員等は、外部で情報処理業務を行う場合には、持ち出す情報資産の重要性分類に応じた情報セキュリティ対策を実施しなければならない。この場合において、教育情報セキュリティ管理者は、その方法を実施手順において明示しなければならない。

５　教職員等は、支給された以外の情報システムの機器及び記録媒体等を持込み、業

務に利用してはならない。ただし、教育情報セキュリティ管理者が業務上必要と認める場合には、その許可を得て利用することができる。

6　教育情報セキュリティ管理者は、前項までに規定する端末等の持出し及び持込みについて、その記録を作成し、保管しなければならない。

7　教職員等は、支給された端末及びソフトウェア等のセキュリティ機能の設定を変更してはならない。

8　教職員等は、校務用端末を含むパソコン、モバイル端末、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閲覧されることがないように、適切な措置を講じなければならない。

9　教職員等は、異動、退職等により学校の所属を離れる場合には、利用していた情報資産を返却しなければならない。

（教育及び訓練）

第21条　教育情報システム管理者は、村情報システム管理者と連携して教職員等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うとともに、教職員等へ周知しなければならない。

2　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。

（セキュリティインシデントの報告）

第22条　教職員等は、情報セキュリティインシデント（事故又は事象）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。

2　前項により報告を受けた教育情報セキュリティ管理者は、速やかに教育情報システム管理者へ報告し、指示を仰がなくてはならない。

3　教職員等は、保護者等外部から情報セキュリティインシデント（事故又は事象）について報告を受けた場合は、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。

4　教育情報セキュリティ管理者は、発生した情報セキュリティインシデントについて、必要に応じＣＩＳＯ及び統括教育情報セキュリティ責任者に事象の発生状況から再発防止策までの詳細について報告しなければならない。

（ＩＤ及びパスワード等の管理）

第23条　教職員等は、自己の管理するＩＣカード等を他者が不正に利用することのできないよう適切に管理しなければならない。

2　教職員等は、自己の保有するパスワードについて、不用意にメモを作成するなどしないよう、パスワードの漏えい防止に努め適切に管理しなければならない。

第６章　技術的セキュリティ対策

（情報システムの管理）

第24条　教育情報システム管理者は、インターネット接続を前提とする校務外部接続系情報及び学習系情報については、外部流出の可能性を考慮し、安全管理措置を講じなければならない。

２　教育情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、適切に管理しなければならない。

３　教育情報システム管理者は、教職員等からのシステム障害の報告、システム障害に関する処理結果又は課題等を記録として保存しなければならない。

（ネットワークの管理）

第25条　教育情報システム管理者は、所管するシステムについて外部ネットワークと接続しようとする場合には教育情報セキュリティ責任者へ報告しなければならない。

２　教育情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、村情報システム管理者へ速やかに報告し、当該外部ネットワークの遮断等の対策を取らなければならない。

３　教育ネットワークは、校務系システム及び学習系システム間の通信経路を物理的又は論理的に分離し、校務系システムについては、インターネットとの接続を制限する等、それぞれに適切な情報セキュリティ対策を講ずるものとする。

４　教育情報システム管理者は、校務系システムと校務外部系システム等その他のシステムとの間で通信する場合には、各システムにおけるアクセス制御等適切な措置を講じなければならない。

５　教職員等は、許可なく支給以外の端末等を教育ネットワークに接続してはならない。

（複合機の管理）

第26条　複合機を教育ネットワークに接続する場合には、原則として当該機器の管理情報送信機能を使用してはならない。

２　統括教育情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体内の情報を抹消又は再利用できないようにする対策を講じなければならない。

（電子メールの利用制限）

第27条　教職員等は、教育ネットワーク用として割当てられた電子メールアカウント（以下、「教育ネットワークメール」という。）を利用することとし、フリーメールサービス等を原則業務に利用してはならない。

２　教職員等は、教育ネットワークメールを村が提供する以外のメールサービス又は

ソフトウェア等へ登録する等、教育情報システム管理者が許可したものを除き、転送をしてはならない。

（ソフトウェアの導入）

第28条　教職員等は、原則として支給された端末等に当初からインストールされていたソフトウェア以外のものをインストールしてはならない。ただし、教育情報セキュリティ管理者が業務上必要と認めた場合には、その限りではない。

２　前項により業務上必要なソフトウェアをインストールする場合には、教育情報システム管理者へ申請し許可を得なければならない。

（機器構成の変更）

第29条　教職員等は、校務用端末及び学習者用端末について、機器の改造及び構成を変更してはならない。

（ウェブの閲覧）

第30条　教職員等は、業務以外の目的でウェブを閲覧してはならない。

２　統括教育情報セキュリティ責任者は、教職員等のウェブ利用について教育情報セキュリティ管理者に対し適切な措置を求めなければならない。

（アクセス制御等）

第31条　教育情報システム管理者は、所管する情報システムごとに権限のない教職員等がアクセスすることのできないよう、システム上制限をしなければならない。

２　教育情報セキュリティ管理者は、業務上システム利用の必要がなくなった教職員等がいる場合には、利用者登録の抹消について教育情報システム管理者に通知しなければならない。

３　教職員等は、外部からの教育系システムへのアクセスをする場合には、適切な情報セキュリティ対策を講じた上で、必要最低限にしなければならない。

（システムの開発、導入及び保守）

第32条　教育情報システム管理者は、所管する情報システムの導入及び移行に当たっては、村情報システム管理者へ報告し、必要な場合には、情報セキュリティ対策について指示を仰がなければならない。

２　教育情報システム管理者は、情報システムの開発、導入及び保守に関する資料及びシステム関連文書を適切に整備・保管しなければならない。

３　教育情報システム管理者は、情報システムの開発、導入及び移行等の際には、既存の教育系システムに影響を与えないよう、事前の検証等を行わなければならない。

（不正プログラム対策）

第33条　教育情報システム管理者は、不正プログラム対策として次の措置を実施しなければならない。

⑴　コンピュータウイルス等の不正プログラムに関する情報を収集し、必要に応じ教職員等への注意喚起を行わなければならない。

⑵　所管するシステムについて、サーバ及びパソコン等の端末へコンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

⑶　不正プログラム対策ソフトウェア及びパターンファイルは、常に最新の状態を保持しなければならない。

⑷　開発元がサポートを終了したソフトウェアを業務利用してはならない。

（教職員等の遵守事項）

第34条　教職員等は、不正プログラム対策として次の措置を実施しなければならない。

⑴　支給された端末等に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には、当該ソフトウェアの設定を変更してはならない。

⑵　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによる検査を行わなければならない。

⑶　教育情報システム管理者が提供する不正プログラムに関する注意喚起等の情報を常に確認しなければならない。

⑷　不正プログラムへの感染が疑われる場合には、速やかに教育情報システム管理者へ報告するとともに、ネットワークから切り離さなければならない。

（不正アクセス対策）

第35条　教育情報システム管理者は、不正アクセス対策として次の措置を実施しなければならない。

⑴　使用されていないポートや不要なサービスについて、閉鎖や機能の停止をしなければならない。

⑵　所管する情報システムに攻撃を受けた際の事実確認及び対策検討に備え、システムの動作記録を保存しなければならない。

⑶　教職員等による教育系システムへの不正アクセスがあった場合は、当該教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に通知し、適切な措置を求めることとする。

（セキュリティ情報の収集）

第36条　教育情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、関係者間で共有しながら必要に応じ対応方法について、教職員等に周知しなければならない。

第７章　運用

（遵守状況の確認）

第37条　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ＣＩＳＯ及び統括教育情報セキュリティ責任者に報告しなければならない。

２　前項により報告を行った場合、その対処方法については村情報セキュリティポリシーに定める野沢温泉村ＣＳＩＲＴ（情報セキュリティ対策組織：Ｃｏｍｐｕｔｅｒ Ｓｅｃｕｒｉｔｙ Ｉｎｃｉｄｅｎｔ Ｒｅｓｐｏｎｓｅ Ｔｅａｍ。以下「村ＣＳＩＲＴ」という。）による検討事項とする。

３　第１項の報告が、重要性分類Ⅰ及びⅡに該当する疑いがある場合、または外部漏えいの可能性がある場合は、直ちに村ＣＳＩＲＴへ通報する。

（端末等の利用状況調査）

第38条　村情報システム管理者及び教育情報システム管理者は、不正アクセス、不正プログラム等の調査のため、教職員等が使用する端末等の利用及び操作の履歴を調査することができる。

（教職員等の報告義務）

第39条　教職員等は、教育情報セキュリティポリシーへの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に報告を行わなければならない。

２　前項により報告を受けた教育情報セキュリティ管理者は、その内容を直ちに教育情報システム管理者に報告しなければならない。

３　前項により報告を受けた教育情報システム管理者は、その内容について必要に応じ教育情報セキュリティ責任者及び村情報システム管理者に報告するとともに、対処方法について協議を行わなければならない。

（緊急時対応計画）

第40条　緊急時のインシデント対応については、村情報セキュリティポリシーに定める緊急時対応計画を適用する。

（法令等遵守）

第41条　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、次の法令の他関係法令等を遵守し、これに従わなければならない。

⑴　地方公務員法（昭和25年法律第261号）

⑵　教育公務員特例法（昭和24年法律第１号）

⑶　著作権法（昭和45年法律第48号）

⑷　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）

⑸　個人情報の保護に関する法律（平成15年法律第57号）

⑹　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）

⑺　サイバーセキュリティ基本法（平成26年法律第104号）

⑻　野沢温泉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１号）

（懲戒処分等）

第42条　教育情報セキュリティポリシーに違反した教職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

第８章　外部サービスの利用

（外部委託の管理）

第43条　教育情報システム管理者は、外部委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

２　教育情報システム管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定しなければならない。

３　教育情報システム管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

４　情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で次の情報セキュリティ要件を明記した契約を締結しなければならない。

⑴　教育情報セキュリティポリシー及び教育情報セキュリティ実施手順の遵守に関する事項

⑵　外部委託事業者の責任者、委託内容、作業者、作業場所の特定に関する事項

⑶　提供されるサービスレベルの保証に関する事項

⑷　外部委託事業者にアクセスを許可する情報の種類と範囲及びアクセス方法に関する事項

⑸　外部委託事業者の従業員に対する教育の実施に関する事項

⑹　提供された情報の目的外利用及び受託者以外の者への提供禁止に関する事項

⑺　業務上知り得た情報の守秘義務に関する事項

⑻　再委託に関する制限事項の遵守に関する事項

⑼　委託業務終了後の情報資産の返還、廃棄等に関する事項

⑽　委託業務の定期報告及び緊急時報告義務に関する事項

⑾　村による検査及び現地調査に関する事項

⑿　村による情報セキュリティインシデントの公表に関する事項

⒀　教育情報セキュリティポリシーが遵守されなかった場合の損害賠償等に関する事項

（約款による外部サービスの利用）

第44条　電子メールやファイルストレージを含む約款による外部サービス利用は、教育情報システム管理者が利用申請を行ったものについてのみ、業務利用を可能とする。

２　前項に規定する外部サービスは、学習系システムでの利用に限定し、校務系システムについては原則として利用を禁止する。

３　教育情報システム管理者は、約款による外部サービスの利用に当たっては急なサービス停止や仕様変更により情報が滅失し復元不可能となる場合に備え、バックアップを取得しなければならない。

（ソーシャルメディアの利用）

第45条　ソーシャルメディアの利用については、村情報セキュリティーポリシーを準用する。その際、公式アカウント開設及び運用管理責任者は教育情報セキュリティ管理者として読み替えるものとする。

２　村情報セキュリティポリシーに規定のない運用の詳細については、別途教育情報セキュリティ管理者が実施手順において定める。

３　重要性分類Ⅲ以上の情報はソーシャルメディアで発信してはならない。

４　利用するソーシャルメディアごとに責任者を定めなければならない。

第９章　１人１台端末におけるセキュリティ対策

（学習者用端末の管理）

第46条　教育情報システム管理者は、学習者用端末でのウェブページの閲覧や不正アクセスについて、適切な措置を講じなければならない。

２　教育情報セキュリティ管理者は、学習者用端末の運用ルールを制定し、安全管理措置を講じなければならない。

３　教職員等は、児童生徒が学習者用端末を紛失した場合、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。

４　前項の規定により報告を受けた教育情報セキュリティ管理者は、速やかに教育情報システム管理者へ報告し、指示を仰がなければならない。

５　教育情報システム管理者は、児童生徒が学習系システムを活用する際にアカウント管理等が煩雑にならないよう対策を講じなければならない。

第 10 章　評価及び見直し

（自己点検）

第47条　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は、教育ネットワーク及び所管するシステムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

２　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、学校内に

おける教育情報セキュリティポリシーに沿った情報セキュリティ対策の実施状況について、毎年度及び必要に応じて自己点検を実施しなければならない。

３　前項までの規定により実施した自己点検結果については、その結果に基づく改善策と併せて取りまとめ、統括教育情報セキュリティ責任者に報告しなければならない。

（見直し）

第48条　統括教育情報セキュリティ責任者は、自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、教育情報セキュリティポリシー及び関係要綱等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めたときは改善を行うものとする。

附　則

この規程は、公布の日から施行する。