錦町立学校教育情報セキュリティポリシー（案）

令和７年　　月

錦町教育委員会

目次

第１章　教育情報セキュリティ基本方針

１　目的

現在、錦町立学校（以下「学校」という。）においては、文部科学省提唱の「ＧＩＧＡスクール構想」に基づき、１人１台の端末及び教育用クラウドサービスの活用を進め、個別に最適化された教育環境において、協同的な学びの充実を推進している。学校が取り扱う情報には、児童生徒、保護者、職員等の個人情報及び学校運営上重要な情報が含まれ、外部への漏洩等が発生した場合、極めて重大な結果を招くおそれがある。

そのため、学校のＩＣＴ環境整備が進むに当たり、不正アクセスや盗難・紛失等、情報資産の保護に向けた十分な情報セキュリティ対策を講じることは、教職員及び児童生徒等が安心してＩＣＴを活用するために必要不可欠である。

また、ＧＩＧＡスクール構想の推進により、クラウドサービスの活用を前提としたネットワーク構成等の課題に対応するとともに、児童生徒等の端末と教職員の端末から得られる各種教育情報を効果的に活用して教育の質的改善を図るため、文部科学省の「教育情報セキュリティポリシーに関するガイドライン（令和７年３月版）」を参考に、錦町教育委員会において「錦町立学校教育情報セキュリティポリシー」（以下「このポリシー」という。）を策定するものとする。

２　構成

このポリシーは、学校が保有する情報資産に対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、学校が保有する情報資産を取り扱う全教職員に浸透、定着させるものであり、安定した統一的規範であることが求められる。一方、情報処理や通信技術の進歩による急速な環境変化に柔軟に対応することも必要であることから、不変的な部分として統一的な規範を定めた「教育情報セキュリティ基本方針」と情報資産を取り巻く環境の変化に柔軟に対応する部分となる「教育情報セキュリティ対策基準」の２部構成として策定する。

〔教育情報セキュリティポリシーの構成〕

文　書	内　容	
錦町立学校教育情報セキュリティポリシー	教育情報セキュリティ基本方針	教育情報セキュリティ対策に関する統一的かつ基本的な方針
	教育情報セキュリティ対策基準	教育情報セキュリティ基本方針を実行にうつすためのすべての教育情報システムに共通の教育情報セキュリティ対策の基準

3　用語の定義

このポリシーにおける用語の定義は、次に定めるところによる。

用　語	定　義
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。
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。
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。
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。
校務系情報	学校が保有する情報資産のうち、それらの情報を学校・学級の運営管理、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、該当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	ネットワーク分離による対策を講じたシステム構成において、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。
学習系情報	学校が保有する情報資産のうち、それらの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、当該情報に教職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。
ネットワーク	コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。インターネットの接続は問わない。
サーバ	ネットワーク上で学校情報を処理し、端末に提供するコンピュータ。
端末機	ネットワークを通じてサーバに接続されたパソコンやモバイル端末（タブレット等）機器。
校務用端末	校務系情報すべてにアクセス可能な端末。
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。
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。
教育情報システム	情報資産を扱うハードウェア、ソフトウェア、クラウドサービス等。
情報セキュリティインシデント	情報セキュリティに関する問題としてとらえられる事象（障害、事件、事故、欠陥、攻撃、侵害等）。
記録媒体	情報システムでデータ等を記録するための媒体（メディア）。サーバ、端末機、デジタルカメラ、デジタルビデオカメラ、通信回線装置等に内蔵される内蔵電磁的記録媒体と、外付けハードディスク、CD-ROM、DVD-R、USB メモリ、SD カード等の外部電磁的記録媒体。
スマートデバイス	情報処理端末（デバイス）のうち、スマートフォンやタブレット等、携行可能な多機能端末。
情報資産	情報システム及びネットワーク並びにこれらで取り扱われる学校情報（これらを印刷した文書も含む）。

無線ＬＡＮ	電波等を利用してデータの送受信を行う構内通信網システム。
クラウド	学校外、庁舎外でプログラムやデータベースを管理し、ネットワークを介してこれを利用する仕組みや概念。
ソーシャルメディアサービス	インターネット上における、ホームページ、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等。
教職員	教育委員会所管の学校に勤務する教職員等。会計年度任用職員を含む。

４　情報資産の分類と管理

学校の情報資産の機密性、完全性及び可用性により、次のとおり分類し、必要に応じて取扱制限を定め、適正な管理を行う。

分類	分　類　基　準
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もの。
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もの。
Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼすもの。
Ⅳ	影響をほとんど及ぼさないもの。

［情報資産の分類］

情報財産の分類		情報資産の例示		
		各情報資産にアクセスする主体		
重要性分類	定義	教職員等・教育委員会	教職員等・教育委員会・児童生徒・保護者	不特定多数
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もの。	**業務に係る特定の教職員等・教育委員会のみがアクセスすることが想定される情報** ○情報システムの設計に関する情報 ・教育情報システム設計書・設定書 ○学校運営に関する情報 ・入学者選抜問題 ・指導要録原本 ・教職員の人事記録 ○健康に関する情報（医師等による指導、診療、調剤の事実等要配慮個人情報を含むもの） ○指導に関する情報（犯罪の経歴、犯罪により害を被った事実、少年法に関する事項等要配慮個人情報を含むもの） ○その他要配慮個人情報を含む情報　　等	**業務に係る特定の教職員等・教育委員会に加えて、児童生徒またはその保護者がアクセスする場合、児童生徒本人の情報のみにアクセスすることが想定される、要配慮個人情報等を含む情報** ○健康に関する情報（医師等による指導・診療・調剤の事実等要配慮個人情報を含むもの） ・健康診断票 ○その他要配慮個人情報を含む情報　等	
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もの。	**業務に係る教職員等・教育委員会のみがアクセスすることが想定される情報** ○情報システムの運用に関する情報 ・システムログイン ID 管理台帳 ・端末ログイン ID 管理台帳 ○学校運営に関する情報（Ⅰを除くもの） ・教職員および児童生徒の、生活歴、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 ○健康に関する情報（医師等による指導、診療、調剤の事実等要配慮個人情報を含まないもの）	**業務に係る教職員等・教育委員会に加えて、児童生徒又はその保護者がアクセスする場合、児童生徒本人の情報のみにアクセスすることが想定される、要配慮個人情報等が含まない情報** ○成績に関する情報 ・通知表 ・定期考査・テスト等の採点結果 ○健康に関する情報（医師等による指導、診療、調剤の事実等要配慮個人情報を含まないもの）　　等	

		・養護教諭・スクールカウンセラー等による記録 ○指導に関する情報（Ⅰを除くもの） ・個別指導計画 ・生徒指導に関する記録 ・家庭訪問や個別面談に関する記録 ○成績に関する情報 ・進級・卒業認定資料 ○進路に関する情報 ・進路希望調査 ・入学者選抜に関する表簿（願書等） ・調査書 ・推薦書 ・卒業生進路先情報 ○学籍に関する情報 ・転退学・転入学・就学・休学等に関する情報 ・教科用図書の給付に関する情報 ○児童生徒の氏名・所属等に関する情報 ・児童生徒名簿、児童生徒住所録 ・保護者緊急連絡網 ・職員緊急連絡網、職員住所録　　等		
Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼすもの。	**教職員等全員・教育委員会がアクセスすることが想定される情報** ○学校運営に関する情報（職員室等で日常的に運用するもので、Ⅱ以上を除くもの） ・職員会議資料 ○児童生徒の氏名・所属等に関する情報（教室等で日常的に運用するもので、Ⅱ以上を除くもの） ・出席簿　　等	**教職員等全員・教育委員会に加えて、児童生徒及び保護者がアクセスすることが想定される情報** ○児童生徒の氏名・所属等に関する情報 ・座席表 ・児童生徒委員会名簿 ○学校運営に関する情報 ・卒業アルバム ・児童生徒の個人写真・集合写真、学校行事等の児童生徒の 写真 ○学習活動の中で生成される情報 ・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、日常的な簡易な健康観察等） ・学習活動の記録（動画・写真等） ○学習指導に関する情報 ・授業用教材、児童生徒用配布プリント等	
Ⅳ	影響をほとんど及ぼさないもの。	**教職員等全員・教育委員会がアクセスすることが想定される、Ⅲ以上を除く情報**	**教職員等全員・教育委員会に加えて、児童生徒及び保護者がアクセスすることが想定される、Ⅲ以上を除く情報**	**不特定多数に公開することが想定される情報** ○学校運営に関する情報（広報等のため活用するもの） ・学校要覧・学校経営案 ・学校・学年・学級だより ・学校ホームページ掲載情報 ○学習活動で生成される情報（保護者の同意等を得て広報等のため活用するもの）　　等

※機密性による情報資産の分類

分　類	分　類　基　準	該当する情報資産のイメージ
機密性３	学校で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	特定の教職員のみが知り得る状態を確保する必要のある情報で秘密文書に相当するもの
機密性２Ｂ	学校で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	教職員のみが知り得る状態を確保する必要がある情報資産（教職員のうち特定の教職員のみが知り得る状態を確保する必要があるものを含む）
機密性２Ａ	学校で取り扱う情報資産のうち、直ちに一般に公表することを前提としていないが、児童生徒等がアクセスすること	教職員及び児童生徒同士のみが知り得る状態を確保する必要がある情報 資産（教職員及び児童生徒のうち特定の教職員及

	を想定している情報資産	び児童生徒のみが知り得る状態を確保する必要があるものを含む)
機密性１	機密性２Ａ、機密性２Ｂ又は機密性３の情報資産以外の情報資産	公表されている情報資産又は公表することを前提として作成された情報資産（教職員及び児童生徒以外の者が知り得ても支障がないと認められるものを含む)

※完全性による情報資産の分類

分　類	分　類　基　準	該当する情報のイメージ
完全性２Ｂ	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の的確な遂行に支障(軽微なものを除く)を及ぼすおそれがある情報資産	情報が正確・完全な状態である必 要があり、破壊、改ざん、破損又 は第三者による削除等の事故があった場合、業務の遂行に支障ある情報
完全性２Ａ	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の的確な遂行に軽微な支障を及ぼすおそれがある情報資産	情報が正確・完全な状態である必 要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合､業務の遂行に軽微な支障ある情報
完全性１	完全性２Ａ又は完全性２Ｂの情報資産以外の情報資産	事故があった場合でも業務の遂行に支障がない情報

※可用性による情報資産の分類

分　類	分　類　基　準	該当する情報のイメージ
可用性２Ｂ	学校で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に支障(軽微なものを除く)を及ぼすおそれがある情報資産	必要な時にいつでも利用できる必要 があり、情報システムの障害等によ る滅失紛失や、情報システムの停止 等があった場合、業務の安定的な遂 行に支障がある情報
可用性２Ａ	学校で取り扱う情報資産のうち､滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に軽微な支障を及ぼすおそれがある情報資産	必要な時にいつでも利用できる必要 があり、情報システムの障害等によ る滅失紛失や、情報システムの停止 等があった場合、業務の安定的な遂 行に軽微な支障がある情報
可用性１	可用性２Ａ又は可用性２Ｂの情報資産以外の情報資産	滅失、紛失や情報システムの停止等 があっても業務の遂行に支障がない 情報

5　教育情報セキュリティ対策

情報資産を脅威から保護するため、次に定める教育情報セキュリティ対策を講ずるものとする。

⑴　管理体制

情報資産を管理し、機密性、完全性及び可用性を維持するための体制を確立する。

⑵　物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・盗難等から保護するために施設整備等の物理的な対策を講ずる。

⑶　人的セキュリティ対策

教育情報セキュリティに関する権限や責任を定めるとともに、全教職員等にこのポリシーを周知徹底するための教育及び啓発を行う等、必要な対策を講ずる。

⑷　技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、不正プログラム対策ソフトウェアの導入等の技術面における対策を講ずる。

⑸　運用

①　情報システムの監視、この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、このポリシーの運用面の対策を講ずる。

②　情報セキュリティが侵害される事態が発生した場合に、被害の拡大防止、復旧等を迅速かつ的確に実施するため、緊急時対応計画を整備する。また、侵害に備えた対応訓練の定期的な実施等の対策を講ずるよう努める。

6　適用範囲

このポリシーの適用範囲は、学校、教育委員会における学校用のシステム、サーバ、クラウドサービス等とする。

7　関係規定

教育情報セキュリティ対策基準を遵守して、教育情報セキュリティ対策を実施するに当たり、その具体的な手順等を明らかにするため、教育委員会及び各学校内で関連規程を定めるものとする。

なお、この規程の中で、公にすることにより学校運営に重大な支障を及ぼすおそれのある情報については、非公開とする。

8　教職員等の責務

学校長、教頭、教職員、会計年度任用職員やその他学校に所属する職員（以下「教職員等」という。）は、情報資産の利用に当たっては、関連法令を遵守しなければならない。また、教職員等は、教育情報セキュリティの重要性を認識し、のポリシーを遵守しなければならない。

９　監査及び点検

このポリシーの遵守状況を検証するため、必要に応じて監査を受け、定期的に点検を実施する。

１０　評価及び見直しの実施

監査又は点検の結果等により、このポリシーに定める事項、及び教育情報セキュリティ対策の評価を行うとともに、情報システムの変更や新たな脅威の発生等、状況の変化に迅速かつ的確に対応するため、必要に応じてこのポリシーの見直しを実施する。

第２章　教育情報セキュリティ対策基準

１　趣旨

この教育情報セキュリティ対策基準は、教育情報セキュリティ基本方針に沿って個々の対策を具体化したものであり、学校における教育情報セキュリティ対策の基準とする。

２　管理体制

教育情報セキュリティの管理体制は以下のとおりとする。

⑴　最高情報セキュリティ責任者（CISO:Chief Information Security Officer、以下「CISO」という。）

①　副町長を、CISO とする。CISO は、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限及び責任を有する。

②　CISO 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情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

③　CISO は、情報セキュリティインシデントに対処するための体制（CSIRT : Computer Security IncIDent Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

④　CISO は最高情報統括責任者（CIO：Chief Information Officer）を兼ねる。

⑵　教育情報統括管理責任者

教育長を CISO 直属の教育情報統括管理責任者とし、学校における全てのネットワークや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統括的な権限及び責任を有する。

⑶　教育情報統括責任者

教育振興課長を教育情報統括責任者とし、学校における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必要かつ十分な措置を行う権限及び責任を有する。

⑷　教育情報セキュリティ管理者

学校教育係長を教育情報セキュリティ管理者とし、学校における情報資産の管理及び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。

⑸　教育情報セキュリティ担当者

学校教育係員を教育情報セキュリティ担当者とし、教育情報セキュリティ管理者（学校教育係長）の指示に従い、学校における情報資産の管理、運用ルールの策定及び情報セキュリティ対策に関する教職員等の教育研修、助言を行う。

⑹　教育情報システム管理者

学校教育係長を教育情報システム管理者とし、学校における教育情報システムの導入、管理、運用、見直し等に関する統括的な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。

⑺　教育情報システム担当者

学校教育係員を教育情報システム担当者とし、教育情報システム管理者（学校教育係長）の指示に従い、学校における教育情報システムの導入、管理、運用、見直し等の作業を行う。また、学校における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管理者（学校教育係長）を補佐する。

⑻　学校教育情報セキュリティ責任者

各学校長を学校教育情報セキュリティ責任者とし、所属校における教育情報セキュリティ実施手順書を策定し、情報資産の管理及び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、学校における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、教育情報セキュリティ管理者（学校教育係長）、教育情報統括責任者（教育振興課長）、教育情報統括管理責任者（教育長）に対する報告義務を定める。

⑼　学校教育情報セキュリティシステム管理者

各学校の教頭を学校教育情報セキュリティシステム管理者とし、学校教育情報セキュリティ責任者（校長）を補佐するとともに、所属する教職員等の教育情報セキュリティ対策の実施について、管理、指導を行う。また、個々の教育情報システムの管理、運用、見直し等の権限及び責任を有する。

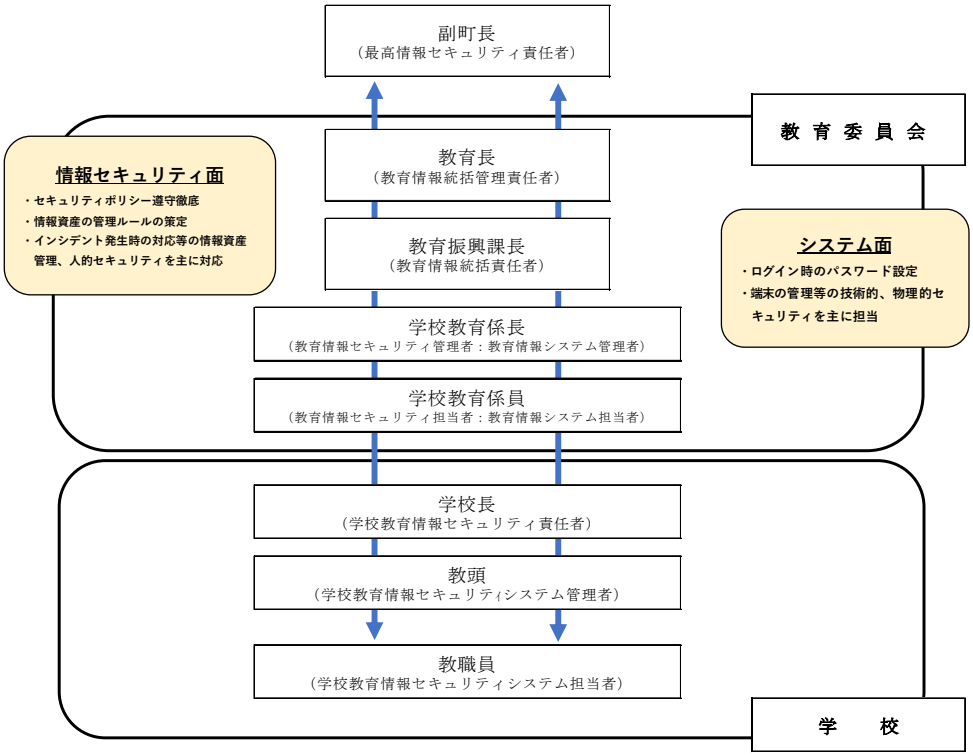
⑽　学校教育情報セキュリティシステム担当者

各学校の情報システムの管理、運用に携わる教職員等を学校教育情報セキュリティシステム担当者とし、管理、運用、見直し等の作業を行う。また、学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）と協力して、全教職員に対しこのポリシーの遵守及び周知・啓発に努める。

⑾　情報セキュリティ委員会への連携

教育情報統括責任者（教育振興課長）は、情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生した事案を正確に把握した上で、情報システム担当課長（総務課長）に報告し、連携を図る。

［教育情報セキュリティ管理体制図］



3　物理的セキュリティ対策

サーバ等や機器の保守・管理、配線や電源等の物理的セキュリティ対策は以下のとおりとする。

⑴　サーバ等の管理

ア　機器の取付け等

①　教育情報システム管理者（学校教育係長）は、サーバ等の機器の取付けを行う場合、地震、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

イ　サーバの冗長化

①　教育情報システム管理者（学校教育係長）は、重要性分類Ⅱ以上の情報資産を格納しているサーバを冗長化し、同一データを保持しなければならない。また、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

②　教育情報システム管理者（学校教育係長）は、重要性分類Ⅲの情報資産を格納しているサーバのハードディスクを冗長化しなければならない。

ウ　機器の電源

①　教育情報システム管理者（学校教育係長）は、教育情報統括責任者（教育振興課長）及び施設管理部門と連携し、重要性分類Ⅱ以上の情報資産を格納しているサーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

②　教育情報システム管理者（学校教育係長）は、教育情報統括責任者（教育振興課長）及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

エ　通信ケーブル等の配線

①　教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

②　教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

③　教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

④　教育情報統括責任者（教育振興課長）、教育情報システム管理者（学校教育係長）は、自ら又は教育情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更又は追加できないように必要な措置を施さなければならない。

オ　機器の定期保守及び修理

①　教育情報システム管理者（学校教育係長）は、重要性分類Ⅲ以上のサーバ等の機器の定期保守を実施しなければならない。

②　教育情報システム管理者（学校教育係長）は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、教育情報システム管理者（学校教育係長）は、外部の事業者に故障を修理さ

せるに当たり、修理を委託する事業者との間で、守秘義務契約を締結するとともに秘密保持体制の確認等を行わなければならない。

カ　施設外又は学校外への機器の設置

教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、施設外又は学校外にサーバ等の機器を設置する場合、CISO（副町長）の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

キ　機器の廃棄等

教育情報システム管理者（学校教育係長）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。

※重要性分類に応じた機器の廃棄等の方法

分　類	機器の廃棄等の方法	確実な履行を担保する方法
（1）重要性分類Ⅰ・Ⅱ	一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である。 具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS 等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	校内等において（2）で後述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。
（2）重要性分類Ⅲ	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。 具体的には、（1）で先述した方法①～⑤のほか、OS 等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。 OS 及び記憶装置の初期化（フォーマット等）による方法は、HDD の記憶演算子にはデータの記憶が残った状態となるため、適当ではない。	校内等において消去を実施し、教職員等が作業完了を確認する方法など適切な方法により確認を行う。

⑵　通信回線及び通信回線装置の管理

ア　通信回線の管理

学校教育情報セキュリティ責任者（校長）は、学校内の通信回線及び通信回線装置を教育委員会と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

イ　外部へのネットワーク接続

学校教育情報セキュリティ責任者（校長）は、外部へのネットワーク接続ポイント及び該当ポイントに接続される端末を正確に把握し、適切な管理を行わなければならない。

ウ　通信回線の適切な選択と情報の暗号化

学校教育情報セキュリティ責任者（校長）は、重要性分類Ⅲ以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、インターネットを通信経路とする回線の場合、通信での暗号化を行わなければならない。

エ　通信回線の暗号化

学校教育情報セキュリティ責任者（校長）は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

⑶　教職員等の利用する端末や電磁的記録媒体等の管理

ア　校務用端末、校務外部接続用端末及び指導者用端末について

①　学校教育情報セキュリティシステム管理者（教頭）は、不正アクセス防止のため、ログイン時の ID 及び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　学校教育情報セキュリティシステム管理者（教頭）は、校務系システム、情報システム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　学校教育情報セキュリティシステム管理者（教頭）は、端末の電源起動時のパスワード(BIOS パスワード、ハードディスクパスワード等）を設定しなければならない。

④　学校教育情報セキュリティシステム管理者（教頭）は、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。

特にパブリッククラウド上で重要な情報（重要性分類Ⅱ以上）を取り扱う際には、多要素認証を含む強固なアクセス制御による対策を講じなければならない。ただし、児童生徒またはその保護者が重要性分類Ⅱ以上の情報資産にアクセスする場合は、児童生徒本人またはその保護者が、当該児童生徒に関するもののみにアクセスすることを想定し

ていることから、多要素認証を設定することが望ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID 及びパスワードでの認証を許容する。

⑤　学校教育情報セキュリティシステム管理者（教頭）は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末に暗号化機能を持つセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。

⑥　学校教育情報セキュリティシステム管理者（教頭）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、重要性分類Ⅲ以上の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。

⑦　学校教育情報セキュリティシステム管理者（教頭）は、モバイル端末の学校外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。

⑧　学校教育情報セキュリティシステム管理者（教頭）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、重要性分類Ⅱ以上の情報資産を取り扱う端末に対し、当該端末の状況およ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。

⑨　学校教育情報セキュリティシステム管理者（教頭）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 Web フィルタリング等の対策を講じなければならない。

イ　学習者用端末について

①　学校教育情報セキュリティシステム管理者（教頭）は、盗難防止のため、教室等で利用するパソコンやモバイル端末の保管庫による管理等の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　学校教育情報セキュリティシステム管理者（教頭）は、情報システム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　学校教育情報セキュリティシステム管理者（教頭）は、授業に支障のないネットワーク構成の選択（帯域や同時接続数等）を行うこと。

④　学校教育情報セキュリティシステム管理者（教頭）は、児童生徒等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）Web フィルタリング、検索エンジンのセーフサーチ、セーフブラウジング

⑤　学校教育情報セキュリティシステム管理者（教頭）は、学校内外での端末におけるマルウェア感染対策を講じなければならない。

⑥　学校教育情報セキュリティシステム管理者（教頭）は、端末のセキュリティ状態の監視に加えて、不適切なアプリケーションやコンテンツを制限し、常に安全で児童生徒等が安心して利用できる状態を維持しなければならない。

⑦　学校教育情報セキュリティシステム管理者（教頭）は、学校内外での端末の運用ルールを制定し、インシデント時の連絡先対応方法を各学校にて整理しなければならない。

⑧　学校教育情報セキュリティシステム管理者（教頭）は、児童生徒が端末を紛失しても、遠隔操作でロックをかける、あるいはワイプ（データ消去）することで第三者による不正操作や情報漏洩を防ぐ等の安全管理措置を講じなければならない。

4　人的セキュリティ

教職員等が情報資産を取扱う際に遵守すべき人的セキュリティ対策は、以下のとおりとする。

⑴　教職員等の遵守事項

ア　教育情報セキュリティポリシー等の遵守

教職員等は、本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、速やかに学校教育情報セキュリティシステム管理者（教頭）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禁止

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。

ウ　モバイル端末や電磁的記録媒体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（本ポリシー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

①　学校教育情報セキュリティ責任者（校長）は、重要分類Ⅱ以上の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

②　教職員等は、学校のモバイル端末、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、学校教育情報セキュリティシステム管理者（教頭）の許可を得なければならない。

③　教職員等は、外部で情報処理業務を行う場合には、学校教育情報セキュリティシステム管理者（教頭）の許可を得なければならない。

エ　支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

①　教職員等は、教職員等は、業務上やむを得ない場合を除いて、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。

②　教職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、学校教育情報セキュリティシステム管理者（教頭）の許可を得た上で、必要な安全管理措置を講じなければならない。

オ　端末等の持ち出し及び持ち込みの記録

学校教育情報セキュリティシステム管理者（教頭）は、端末等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。

カ　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、学校教育情報セキュリティシステム管理者（教頭）の許可なく変更してはならない。

キ　机上の端末等の管理

教職員等は、パソコン、モバイル端末、電磁的記録媒体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、又は学校教育情報セキュリティシステム管理者（教頭）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電磁的記録媒体、文書等の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。

ク　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得た情報を漏らしてはならない。

ケ　情報セキュリティポリシー等の掲示

学校教育情報セキュリティ責任者（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できるように掲示しなければならない。

コ　外部委託事業者に対する説明

学校教育情報セキュリティシステム管理者（教頭）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。

⑵　研修・訓練

ア　学校教育情報セキュリティ責任者（校長）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。

イ　学校教育情報セキュリティ責任者（校長）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、教育委員会の承認を得なければならない。

ウ　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しなければならない。

エ　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。

オ　緊急時対応訓練

学校教育情報セキュリティ責任者（校長）は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

カ　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。

⑶　情報セキュリティインシデントの報告

ア　学校内からの情報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、速やかに学校教育情報セキュリティ責任者（校長）に報告しなければならない。

②　報告を受けた学校教育情報セキュリティ責任者（校長）は、速やかに教育情報セキュリティ管理者（学校教育係長）に報告しなければならない。

③　教育情報セキュリティ管理者（学校教育係長）は、報告のあった情報セキュリティインシデントについて、必要に応じて教育情報統括責任者（教育振興課長）及び教育情報統括管理責任者（教育長）に報告しなければならない。

イ　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

①　教職員等は、管理対象のネットワーク及び教育情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、学校教育情報セキュリティ責任者（校長）に報告しなければならない。

② 報告を受けた学校教育情報セキュリティ責任者（校長）は、速やかに教育情報セキュリティ管理者（学校教育係長）に報告しなければならない。

③ 教育情報セキュリティ管理者（学校教育係長）は、当該情報セキュリティインシデントについて、速やかに教育情報統括責任者（教育振興課長）及び教育情報統括管理責任者（教育長）に報告しなければならない。

④ 教育情報統括責任者（教育振興課長）は、教育情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

ウ 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

① 教育情報統括責任者（教育振興課長）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（学校教育係長）、教育情報システム管理者（学校教育係長）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、教育情報統括管理責任者（教育長）に報告しなければならない。

② 教育情報統括管理責任者（教育長）は、教育情報統括責任者（教育振興課長）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。

⑷ ID 及びパスワード等の管理

教職員等は、学校情報教育セキュリティ責任者（校長）が許可をした者を除いて、次の事項を厳守しなければならない。

ア 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 は、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。

③ 教職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、学校教育情報セキュリティ責任者（校長）又は学校教育情報セキュリティシステム管理者（教頭）に通知しなければならない。

イ 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ければならない。

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、学校教育情報セキュリティ責任者（校

長）に速やかに報告し、パスワードを速やかに変更しなければならない。

⑤　複数の教育情報システムを扱う教職員等は、同一のパスワードを複数のシステム間で用いてはならない。（シングルサインオンを除く。）

⑥　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。

⑦　教職員等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。）

⑧　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。

⑸　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等を利用させるに当たり、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　ウイルス対策ソフトウェアの管理

ウイルス対策ソフトウェアは常に最新の状態に保つこと。

④　端末のソフトウェアに関するセキュリティ機能の設定変更禁止

利用する端末のセキュリティ機能の設定を、許可なく変更してはならないこと。

⑤　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。

⑥　無断で外部ソフトウェアをインストール禁止

無断で外部ソフトウェアをインストールしないようにすること。

⑦　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。

⑧　ウイルス感染が疑われる場合の報告

学習用端末が動かない、勝手に操作されている、いつもと異なる画面や警告が表示されるなどの症状がでた場合、すぐに担任教員に報告すること。

⑨　端末の安全な取り扱い

学習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。

⑩　私物端末など許可されていない端末の利用禁止

私物端末など許可されていない端末を学校に持ち込んで、学校のネットワークにつな

がないこと。

⑪　重要性分類Ⅱ以上の情報資産（児童生徒本人の情報に限る）の管理

該当資産を端末にダウンロードした場合には、目的を達成し次第すみやかに消去を行う等の対策を講じること。また、該当資産を閲覧する際には、離席時に端末ロックし、周囲に他の児童生徒がいる状態では閲覧しない等の対策を講じること。

⑹　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得た情報を漏らしてはならない。

5　技術的セキュリティ

情報システム等の不正利用を防止し、不正利用に対する証拠の保全をするための技術的セキュリティ対策は以下のとおりとする。

⑴　コンピュータ及びネットワークの管理

ア　文書サーバ及び端末の設定等

①　教育情報システム管理者（学校教育係長）は、教職員等が使用できる文書サーバの容量を設定し、教職員等に周知しなければならない。

②　教育情報システム管理者（学校教育係長）は、文書サーバを学校等の単位で構成し、教職員等が他の学校等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

③　教育情報システム管理者（学校教育係長）は、住民の個人情報、人事記録等、特定の教職員等しか取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一学校等であっても、担当職員以外の教職員等が閲覧及び使用できないようにしなければならない。

④　教育情報システム管理者（学校教育係長）は、インターネット接続を前提とする校務外部接続系サーバ及び学習系サーバに保管する情報（学習系サーバにおいては、機微な個人情報を保管する場合に限る。）については、標的型攻撃等によるデータの外部流出の可能性を考慮し、データ暗号化等による安全管理措置を講じなければならない。

イ　バックアップの実施

教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、ファイルサーバ等に記録された情報について、サーバの安定な運用対策に関わらず、校務系情報及び校務外部接続系情報、学習系情報について、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。

ウ　他団体との情報システムに関する情報等の交換

教育情報システム管理者（学校教育係長）は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、教育情報統括管理責任者（教育長）及び教育情報統括責任者（教育振興課長）の許可を得なければならない。

エ　システム管理記録及び作業の確認

① 教育情報システム管理者（学校教育係長）は、所属する教育情報システムの運用において実施した作業について、作業記録を作成しなければならない。

② 教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）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、詐取、改ざん等をされないように適切に管理しなければならない。

③ 教育情報統括責任者（教育振興課長）、教育情報システム管理者（学校教育係長）又は教育情報システム担当者（学校教育係員）及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、作業報告書等をもって、その作業を確認しなければならない。

オ　情報システム仕様書等の管理

教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、ネットワーク構成図、情報システム仕様書等について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

カ　ログの取得等

① 教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

② 教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

③ 教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について、点検又は分析を実施しなければならない。

キ　障害記録

教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、教職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

ク　ネットワークの接続制御、経路制御等

①　教育情報統括責任者（教育振興課長）は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

②　教育情報統括責任者（教育振興課長）は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

ケ　外部ネットワークとの接続制限等

①　教育情報システム管理者（学校教育係長）は、所管するネットワークを外部ネットワークと接続しようとする場合には、教育情報統括責任者（教育振興課長）の許可を得なければならない。

②　教育情報システム管理者（学校教育係長）は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁舎内及び学校の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

③　教育情報システム管理者（学校教育係長）は、接続した外部ネットワークの瑕疵によりデータの漏洩、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

④　教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、ウェブサーバ等をインターネットに公開する場合、教育ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

⑤　教育情報システム管理者（学校教育係長）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、教育情報統括責任者（教育振興課長）の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

コ　無線ＬＡＮ及びネットワークの盗聴対策

①　教育情報統括責任者（教育振興課長）は、無線ＬＡＮの利用を認める場合、解読が困難な通信の暗号化及び認証技術の使用を義務付けなければならない。

②　教育情報統括責任者（教育振興課長）は、機密性の高い情報を取扱うネットワークについて、情報の盗聴等を防ぐため、通信の暗号化等の措置を講じなければならない。

サ　電子メールのセキュリティ管理

①　教育情報統括責任者（教育振興課長）は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、

電子メールサーバの設定を行わなければならない。

② 教育情報統括責任者（教育振興課長）は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

③ 教育情報統括責任者（教育振興課長）は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④ 教育情報統括責任者（教育振興課長）は、教職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を教職員等に周知しなければならない。

⑤ 教育情報統括責任者（教育振興課長）は、システム開発や運用、保守等のため施設内に常駐している外部委託事業者の作業員による電子メールアドレス利用につい て、外部委託事業者との間で利用方法を取り決めなければならない。

⑥ 教育情報統括責任者（教育振興課長）は、教職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置しなければならない。

シ 電子メールの利用制限

① 教職員等は、電子メールと転送機能を用いて、個人所有の電子メールに転送してはならない。

② 教職員等は、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。

③ 教職員等は、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。

④ 教職員等は、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（学校教育係長）に報告しなければならない。

⑤ 教職員等は、ウェブで利用できるフリーメールサービス等を教育情報統括責任者（教育振興課長）の許可なしに使用してはならない。

⑥ 教職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、暗号化又はパスワード設定等、セキュリティを考慮して送信しなければならない。

⑦ 児童生徒等が扱う電子メールは、学校教育情報セキュリティ責任者（校長）が許可した相手だけに送受信できる設定にしなければならない。

ス 無許可ソフトウェアの導入等の禁止

① 教職員等は、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。

② 教職員等は、業務上の必要がある場合は、教育情報セキュリティ管理者（学校教育係長）及び教育情報システム管理者（学校教育係長）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（学校教育係長）又は教育情報システム管理者（学校教育係長）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。

③　教職員等は、不正に入手したソフトウェアを利用してはならない。

セ　機器構成の変更制限

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、教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）の許可を得なければならない。

ソ　無許可でのネットワーク接続の禁止

教職員等は、学校教育情報セキュリティ責任者（校長）の許可なく、パソコンやモバイル端末をネットワークに接続してはならない。

タ　業務以外の目的でのウェブ閲覧の禁止

①　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　学校教育情報セキュリティ責任者（校長）は、教職員等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（学校教育係長）に通知し、適切な措置を求めなければならない。

チ　無線ＬＡＮ及び移動体通信の利用制限

教職員等は、学校教育情報セキュリティ責任者（校長）が認めた場合に限り、教育外部系（授業用）ネットワーク、新教育外部系ネットワークの無線ＬＡＮ及び移動体通信を利用することができる。

ツ　スマートデバイスに係るセキュリティ管理

①　学校教育情報セキュリティシステム管理者（教頭）は、スマートデバイスが備える機能や使用環境、取扱う情報、その他業務の特性等に応じ、適正なセキュリティ要件を定め、必要な対策を実施しなければならない。

②　教職員等は、スマートデバイスを使用するにあたり、学校教育情報セキュリティシステム管理者（教頭）等が実施したセキュリティ対策及び、使用手順に従い適正にスマートデバイスを使用しなければならない。

テ　クラウドサービス、ソーシャルメディア利用制限

①　強固なアクセス制御による対策を講じたシステム構成でない場合、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。

②　私的に契約したクラウドサービスや個人アカウントを業務利用してはならない。

③　ソーシャルメディアサービスを利用して、業務上知り得た情報を公開してはならな

い。

⑵　アクセス制御等

ア　アクセス制御等

学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、所管するネットワーク又は情報システムごとに、アクセス権限のない教職員等がアクセスできないように、システム上制限しなければならない。

イ　利用者 ID の取扱い

①　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、利用者の登録、変更、抹消等の情報管理、教職員等の異動、出向、退職に伴う利用者 ID の取扱い等の方法を定めなければならない。

②　教職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）に通知しなければならない。

③　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、利用されていない ID が放置されないよう、関係機関と連携し、点検しなければならない。

ウ　特権を付与された ID の管理等

①　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏洩等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

②　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、教育情報統括責任者（教育振興課長）が許可した者を除き、特権を付与された ID 及びパスワードの変更について、外部委託事業者に行わせてはならない。

③　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、特権を付与された ID 及びパスワードについて、その利用期間に合わせて特権 ID を作成・削除する、もしくは、入力回数制限を設ける等のセキュリティ機能を強化しなければならない。

④　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、特権を付与された ID を、初期設定以外のものに変更しなければならない。

エ　教職員等による外部からのアクセス等の制限

①　教職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）の許可を得なければならない。

②　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

⑤　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、外部からのアクセスに利用するモバイル端末を教職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑥　教職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を施設内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、学校教育情報セキュリティシステム管理者（教頭）に報告しなければならない。

⑦　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、公衆通信回線（公衆無線ＬＡＮ等）を教育ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者の ID 及びパスワード、生体認証に係る情報等の認証情報等による認証に加えて、通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

オ　パスワードに関する情報の管理

①　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）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。

②　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、教職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

カ　特権による接続時間の制限

学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

⑶　システム開発、導入、保守等

ア　情報システムの調達

①　教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

②　教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

イ　情報システムの開発

①　教育情報システム管理者（学校教育係長）は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発を行う場合には、教育情報統括責任者（教育振興課長）に協議しなければならない。

②　教育情報システム管理者（学校教育係長）は、システム開発に当たって、リスク分析を行うとともに、事故、障害等による被害の発生を防止する、もしくは最小限に抑えるため、必要な対策を講じなければならない。

ウ　情報システムの導入

①　教育情報システム管理者（学校教育係長）は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に、十分なテストを行い、不具合の発見及び解消に努めなければならない。

②　教育情報システム管理者（学校教育係長）は、個人情報及び機密性の高いデータを、テストデータに使用してはならない。

③　教育情報システム管理者（学校教育係長）は、既存のネットワークを利用したシステムを導入しようとするときは、ネットワークへの接続テストを行うとともに、アクセス権限を明確にし、アクセスの管理等に関する事項を定めなければならない。

エ　システム開発、保守に関連する資料等の整備、保管

教育情報システム管理者（学校教育係長）は、システム開発・保守に関連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。

オ　開発、保守用のソフトウェアの更新等

教育情報システム管理者（学校教育係長）は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

カ　システム更新又は統合時の検証等

教育情報システム管理者（学校教育係長）は、システム更新、統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新、統合後の業務運営体制の検証を行わなければならない。

⑷　不正プログラム対策

ア　学校教育情報セキュリティ責任者（校長）の措置事項

学校教育情報セキュリティ責任者（校長）は、不正プログラム対策として、次の事項を措置しなければならない。

①　外部ネットワークから受信したファイルは、ウイルス対策ソフト等を使用し、コンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

②　外部ネットワークに送信するファイルは、ウイルス対策ソフト等を利用し、コンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③　コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ教職員等に対して注意喚起しなければならない。

④　所掌するサーバ及びパソコン等の端末に、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。

⑤　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、常に最新の状態に保たなければならない。

⑥　業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

イ　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。

②　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チェックを行わなければならない。

③　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。

④　端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実

施しなければならない。

⑤　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

⑥　不正プログラム対策ソフトウェア開発者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。

⑦　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、以下の対応を行い、速やかに教育情報セキュリティ管理者（学校教育係長）に報告しなければならない。

・パソコン等の端末の場合は、ＬＡＮケーブルの即時取り外しを行わなければならない。

・モバイル端末の場合は、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　専門家の支援体制

教育情報統括責任者（教育振興課長）は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

⑸　不正アクセス対策

ア　学校教育情報セキュリティ責任者（校長）は、不正アクセス対策として、以下の事項を措置しなければならない。

①　使用されていないポートや不要なサービスについて、ポート閉鎖や機能を削除又は停止しなければならない。

②　重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

③　教育委員会及び情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

イ　学校教育情報セキュリティ責任者（校長）は、情報システムに対する攻撃予告があり、攻撃を受けることが明確になった場合には、システムの停止を含む必要な措置を講じなければならない。また、教育委員会との連絡を密にし、情報の取集に努めなければならない。

ウ　学校教育情報セキュリティ責任者（校長）は、外部からサーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び教育委員会との緊密な連携に努めなければならない。

エ　教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、教職員等及び外部委託事業者が使用しているパソコンやモバイル端末からのネットワークやサーバ等に対する攻撃や、外部のサイトに対する攻撃を監視しなければならない。

オ　教育情報統括責任者（教育振興課長）は、教職員等が学校内にあるパソコンやモバイル端末を利用した不正アクセスを発見した場合には、当該教職員等が所属する学校教育情報セキュリティ責任者（校長）に通知し、適切な措置を求めなければならない。

カ　学校教育情報セキュリティ責任者（校長）は、標的型攻撃による内部への侵入を防止するために、以下のような対策を講じなければならない。

①　人的対策（標的型攻撃メール対策）

・差出人に心当たりのないメールは開封しない。
・不自然なメールが着信した際は、差出人にメール送信の事実を確認する。
・メールを開封した後で標的型攻撃と気付いた場合、添付ファイルは絶対開封せず、メールの本文に書かれたＵＲＬもクリックしない。
・標的型攻撃と気付いた場合、学校教育情報セキュリティ責任者（校長）に対して着信の事実を報告し、組織への注意喚起を依頼した後に、メールを速やかに削除する。
・学校教育情報セキュリティシステム管理者（教頭）は、メールやログを確認し、不正なメールがなかったかチェックする。（事後対策）

②　電磁的記録媒体に対する対策

・出所不明の電磁的記録媒体を内部ネットワーク上の端末に接続させない。
・電磁的記録媒体をパソコン等の端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。
・パソコン等の端末について、自動再生（オートラン）機能を無効化する。
・パソコン等の端末について、電磁的記録媒体内にあるプログラムを媒体内から直接実行することを拒否する。

⑹　セキュリティ情報の収集

ア　教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、セキュリティホールに関する情報を収集し、必要に応じ、学校と共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェアの更新等の対策を実施しなければならない。

イ　教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、不正プログラム等のセキュリティ情報を収集し、必要に応じ、対処方法について教職員等に周知しなければならない。

ウ　教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、情報セキュリティに関する情報を収集し、必要に応じ、学校と共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって、新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

6　運用

⑴　情報システムの監視

ア　教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。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、重要性分類Ⅱ以上の情報資産へのアクセスについては、侵入検知システム（IDS）や侵入防御システム（IPS）などの端末・サーバ・通信の監視・制御等によるセキュリティ対策を講じなければならない。

イ　学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

ウ　教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）が指名した者は、重要性分類Ⅱ以上の情報資産を格納するシステムを常時監視しなければならない。

エ　教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）が指名した者は、重要性分類Ⅲの情報資産を格納するシステムを常時監視しなければならない。

⑵　教育情報セキュリティポリシーの遵守状況の確認

ア　教育情報統括責任者（教育振興課長）及び教育情報セキュリティ管理者（学校教育係長）は、このポリシーに基づき、情報システム及びネットワークにおける情報セキュリティ対策の実施に関し、必要となる事項を定めた関係規程を作成し、教育情報統括管理責任者（教育長）の承認を得なければならない。

イ　教育情報統括責任者（教育振興課長）及び教育情報セキュリティ管理者（学校教育係長）は、この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、速やかに教育情報統括管理責任者（教育長）に報告し、適切に対処しなければならない。

ウ　教育情報統括責任者（教育振興課長）及び教育情報セキュリティ管理者（学校教育係長）は、ネットワーク及びサーバ等のシステム設定時におけるこの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。

⑶　パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）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、教職員等が業務で利用しているパソコン、モバイル端末及び電磁記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

⑷　教職員等の報告義務

ア　教職員等は、このポリシーに対する違反行為を発見した場合、直ちに学校教育情報セキュリティ責任者（校長）及び学校教育情報セキュリティシステム管理者（教頭）に報告を行わなければならない。

イ　アの違反行為が、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教育情報統括責任者（教育振興課長）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。

⑸　侵害時の対応等

ア　緊急時対応計画の策定

教育情報統括責任者（教育振興課長）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　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

ウ　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、当該計画とこのポリシーの整合性を確保しなければならない。

エ　緊急時対応計画の見直し

教育情報統括責任者（教育振興課長）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。

⑹　例外措置

ア　例外措置の許可

教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、情報セキュリティ関係規程を遵守することが困難な状況で、学校事務及び教育活動の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、教育情報統括管理責任者（教育長）の許可を得て、例外措置を取ることができる。

イ　緊急時の例外措置

教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、学校事務及び教育活動の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに教育情報統括管理責任者（教育長）に報告しなければならない。

ウ　例外措置の申請書の管理

教育情報統括責任者（教育振興課長）及び教育情報システム管理者（学校教育係長）は、例外措置の申請書及び審査結果を適切に保管しなければならない。

⑺　法令等遵守

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。

・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）
・サイバーセキュリティ基本法（平成２６年法律第１０４号）
・錦町情報公開条例（平成１４年錦町条例第２１号）
・錦町個人番号の利用及び特定個人情報の提供に関する条例（平成２７年錦町条例第２１号）
・錦町個人情報保護法施行条例（令和５年錦町条例第１号）

⑻　懲戒処分等

ア　教育情報統括責任者（教育振興課長）は、教職員等がこのポリシーに規定する事項及び指示に違反した場合には、当該教職員等が所属する学校教育情報セキュリティ責任者（校長）に通知し、ネットワーク及び情報機器等の利用を停止し、その権利を剥奪することができる。

イ　当該教職員等は、違反の重大性、発生した事案の状況等に応じて、地方公務員法をはじめとする関係法令による懲戒処分の対象とする。

7　外部委託

⑴　外部委託事業者の選定基準

教育情報システム管理者（学校教育係長）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、事業者を選定しなければならない。

⑵　契約項目

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必要に応じて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。

・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
・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
・提供されるサービスレベルの保証
・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、アクセス方法
・外部委託事業者の従業員に対する教育の実施
・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の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・町による監査、検査
・町による情報セキュリティインシデント発生時の公表
・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規定（損害賠償等）

⑶　確認・措置等

教育情報システム管理者（学校教育係長）は、外部委託事業者において、必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、前項の契約に基づき措置しなければならない。また、その内容を教育情報統括責任者（教育振興課長）に報告するとともに、その重要度に応じて教育情報統括管理責任者（教育長）に報告しなければならない。

⑷　約款による外部サービスの利用

ア　約款による外部サービスの利用に係る規定の整備

①　教育情報システム管理者（学校教育係長）は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、機密性の高い情報が取扱われないように規定しなければならない。

・約款によるサービスを利用してよい範囲

・業務により利用する約款による外部サービス

・利用手続及び運用手順

②　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、約款において以下の点が規定されていることを確認しなければならない。

・利用者が登録した情報が、利用者の同意なく無断使用（目的外利用、第三者への提供等）されないこと

・サービス事業者が業務上知り得た情報の守秘義務が守られること

イ　約款による外部サービスの利用における対策の実施

教職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で、約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

⑸　ソーシャルメディアサービスの利用

ア　教育情報システム管理者（学校教育係長）は、教育委員会又は学校が管理するアカウントで、ソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

①　教育委員会又は学校のアカウントによる情報発信が、実際のものであることを明らかにするために、本町の自己管理ウェブサイトやプロフィール画面等に当該情報を掲載して参照可能とするとともに、アカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

②　パスワードや認証のためのコード等の認証情報等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

イ　機密性２Ａ以上の情報は、ソーシャルメディアサービスで発信してはならない。

ウ　利用するソーシャルメディアサービスごとの責任者を定めなければならない。

8　事業者に対して確認すべきプライバシー保護に関する事項

外部委託やクラウドサービスの利用に当たり、個人情報の収集・利用範囲や管理期間、データの統制と所有の在り方等について、以下の事項について事業者に確認しなければならない。

⑴　個人情報の利用範囲

教育、学校の目的に必要な情報、又は児童生徒等及び保護者の許可した情報を超えて個人情報の収集、維持、使用、共有をしないこと。

⑵　個人情報の無断提供

クラウドサービスの導入によって知り得た個人情報について、売買も含め、無断提供をしないこと。

⑶　個人情報を利用した利用者に対する広告活動等の無断使用の禁止

教育、学校の目的を達成すること以外に、個人情報について児童生徒等及び保護者に対する行動ターゲティング広告をはじめとする、広告活動その他無断使用をしないこと。

⑷　不必要な個人プロファイル作成禁止

教育、学校の目的を達成するため、又は児童生徒等及び保護者によって許可された場合を除き、不必要な個人プロファイルを作成しないこと。

⑸　不適切なポリシー等の変更の禁止

クラウドサービスの運用等において、利用者に対する明確な通知、相談等の対応もなく、利用者のプライバシーポリシーに重大な影響を与えるような変更を行わないこと。

⑹　個人情報の保持期間定義

サービス提供期間（利用者と合意した期間）を超えて個人を特定する情報を保持しないこと。

⑺　個人情報の利用目的

個人情報を収集、使用、共有及び保持するのは、教育機関、教職員、又は利用者によって承認された目的に限ること。

⑻　個人情報の取扱いについての情報開示

個人情報の取扱いについて、契約又はプライバシーポリシーで明確に示すこと。

⑼　利用者による個人情報管理

個人情報の登録、変更、削除に関するサービスを利用者に提供すること。

⑽　個人情報の適正管理

個人情報に対する不正アクセス又は個人情報の紛失、破壊、改ざん、漏洩、盗難等のリスクに対し、適切な安全対策を講じること。また、個人情報を正確かつ最新の状態で管理すること。

⑾　再委託

サービス提供の全部又は一部を第三者に再委託、又は代行実施させる場合には、個人情報保護法制等を遵守し、当該再委託先又は代行実施先について、同等の義務を課し、管理すること。

⑿　合併・買収

合併又は他社による買収を伴う場合、後継企業が以前に収集した個人情報について、同様の義務を負うことを条件に、個人情報を継続して管理するものとすること。

9　点検・評価・見直し

⑴　実施方法

教育情報統括責任者（教育振興課長）及び学校教育情報セキュリティ責任者（校長）は、所管する教育情報システム及び教育ネットワーク等の情報資産における情報セキュリティ対策状況について、定期的又は必要に応じて、点検を行わなければならない。また、外部委託事業者に委託している場合、外部委託事業者から下請けとして受託している事業者も含めて、このポリシーの遵守について、定期的に又は必要に応じて、点検を行わなければならない。

⑵　報告

教育情報統括責任者（教育振興課長）及び学校教育情報セキュリティ責任者（校長）は、情報セキュリティ対策状況についての点検結果を教育情報統括管理責任者（教育長）に報告する。

⑶　保管

教育情報統括責任者（教育振興課長）及び学校教育情報セキュリティ責任者（校長）は、点検の実施を通して収集した点検結果、点検報告書作成のための調書等を、紛失等が発生しないように適切に保管しなければならない。

⑷　点検結果への対応

教育情報統括責任者（教育振興課長）及び学校教育情報セキュリティ責任者（校長）は、点検結果に基づき、必要な改善を行わなければならない。また、点検結果において、このポリシーの記載事項に疑義が生じた場合には、速やかに教育情報統括管理責任者（教育長）に報告し、対処しなければならない。

⑸　教育情報セキュリティポリシー及び関係規程等の見直し・変更

ア　教育情報統括管理責任者（教育長）及び教育情報統括責任者（教育振興課長）は、新たに必要な対策が発生した場合又は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、このポリシー及び関係規程等について、定期的に又は必要に応じて評

価を行い、必要があると認めた場合、見直し、変更等を行わなければならない。

イ　教育情報統括管理責任者（教育長）及び教育情報統括責任者（教育振興課長）は、教育情報セキュリティ対策基準の変更を行った場合には、速やかに学校教育情報セキュリティ責任者（校長）及びその他関係者に周知を行わなければならない。

ウ　教育情報統括責任者（教育振興課長）は、所管する教育情報システム及び教育ネットワーク等について、このポリシーの変更並びに情報セキュリティに関する状況の変化等に応じて、適宜情報セキュリティ対策の見直しを行い、必要があると認めた場合、当該システム及びネットワークの関係規程の変更を行わなければならない。