池田市立学校
教育情報セキュリティポリシー

令和８年３月

池田市教育委員会

〈 目　　次 〉

第１章　教育情報セキュリティ基本方針

1　目的

池田市立幼稚園型認定こども園、小学校、中学校及び義務教育学校（以下「学校」という。）においては、文部科学省の「ＧＩＧＡスクール構想」に基づき、１人１台端末の整備、クラウドサービスの活用を進め、個別最適な学びと協働的な学びを一体的に充実させることが可能となった。

学校には、児童生徒、保護者、教職員の個人情報及び学校運営上重要な情報が多数含まれ、外部への漏えい等が発生した場合、二次被害も含め、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環境整備が進むにあたり、不正アクセス、ウイルス攻撃や部外者の侵入等の意図的な要因による情報資産（校務系情報・学習系情報）の漏えい・破壊・改ざん・消去等、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、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）」、池田市の「池田市情報セキュリティポリシー（令和７年３月版）」を参考に、池田市教育委員会において「池田市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、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ることから、安定した統一的な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の変化に柔軟に対応することも必要であることから、情報セキュリティ対策における統一的な規範として基本的な考え方を定める「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していくための「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。

なお、学校に敷設されている行政系ネットワークの取り扱いについては、「池田市情報セキュリティポリシー」に準拠するものとする。

3　用語の定義

(1)　ネットワーク

学校、教育委員会等における学校用の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。

(2)　情報資産

学校が保有する校務系情報・学習系情報をいう。

(3)　校務系情報

教職員が学校・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。

(4)　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の外部と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をいう。

(5)　学習系情報

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をいう。

(6)　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。

(7)　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及び教育情報セキュリティ対策基準をいう。

(8)　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。

(9)　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。

(10) 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。

(11) サーバ

ネットワーク上で情報資産を処理し、端末に提供するコンピュータをいう。

(12) 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）機器をいう。

(13) 校務用端末

校務系情報全てにアクセス可能な端末をいう。

(14) 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。

(15) 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。

(16) 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をいう。

(17) 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）をいう。

(18) 記録媒体

教育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てい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をいう。

(19) 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をいう。

(20) クラウド

学校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をいう。

(21) 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、動画共有サイト等をいう。
(22) 教職員
学校長、園長、副校長、教頭、副園長、教職員、会計年度任用職員やその他学校に所属する職員をいう。

4 対象とする脅威

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) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器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、火災等の災害によるサービス及び業務の停止等
(4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
(5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

5 適用範囲

このポリシーが対象とする情報資産は、次のとおりとする。

(1) ネットワーク、教育情報システム及びこれらに関する設備、電磁的記録媒体
(2) 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) 教育情報システムの仕様書及びネットワーク図等のシステム関連文書

6 教職員の遵守義務

教職員は､情報セキュリティの重要性について共通の認識を持ち､情報資産の利用にあたっては、関係法令を遵守しなければならない。また、教職員は、情報セキュリティの重要性を認識し、このポリシーを遵守しなければならない。

7 情報セキュリティ対策

上記４の脅威から情報資産を保護するために、以下の対策を講じる。

(1) 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。
(2) 情報資産の分類と管理
情報資産を機密性､完全性及び可用性に応じて分類し､該当分類に基づき情報セキュリティ対策を実施する。
(3) 物理的セキュリティ対策
サーバ、通信回線及び校務用端末等の管理について、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

教育情報システムの監視、このポリシーの遵守状況の確認、業務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じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(7)　業務委託と外部サービスの利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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確認し、必要に応じて契約に基づき措置を講じる。 外部サービスを利用する場合には、利用に係る規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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る。

8　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。

9　このポリシーの見直し

情報セキュリティ監査及び自己点検の結果、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、このポリシーを見直す。

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を実行に移すための学校における情報セキュリティ対策の基準を定めたものである。

2　管理体制

情報セキュリティの管理体制は以下のとおりとする。

(1)　教育情報統括管理責任者

教育長を教育情報統括管理責任者とし､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。

(2)　教育情報統括責任者

教育部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。

(3)　教育情報セキュリティ管理者

教育委員会内の該当課長を教育情報セキュリティ管理者とし､該当課に関する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。

(4)　教育情報セキュリティ担当者

教育委員会内の該当課職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の指示に従い、該当課に関する情報資産の管理、運用ルールの策定及び教育情報セキュリティ対策に関する教職員の教育研修、助言を行う。

(5)　教育情報システム管理者

教育センター所長を教育情報システム管理者とし、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､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。

(6)　教育情報システム担当者

教育センター職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の指示等に従い、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、教育情報システム管理者を補佐する。

(7)　校内教育情報セキュリティ責任者

各学校長及び副校長を校内教育情報セキュリティ責任者とし､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、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システム管理者、教育情報統括責任者、教育情報統括管理責任者に対する報告義務を定める。

(8)　校内教育情報セキュリティ管理者

各学校の教頭を校内教育情報セキュリティ管理者とし､校内教育情報セキュリティ責任者を補佐するとともに､所属する教職員の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。

(9)　校内教育情報システム担当者

各学校の教育情報システムの管理､運用に携わる教職員を校内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、校内教育情報セキュリティ責任者及

び校内教育情報セキュリティ管理者と協力して、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。

3　情報資産の分類と管理

(1)　情報資産の分類

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切な管理を行う。

機密性による情報資産の分類

分類	分類基準	必要な措置
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	・支給以外の端末での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化･パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性２	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	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	

完全性による情報資産の分類

分類	分類基準	必要な措置
完全性２	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	・バックアップ ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性１	完全性２情報資産以外の情報資産	

可用性による情報資産の分類

分類	分類基準	必要な措置
可用性２	学校で取り扱う情報資産のうち、滅失、紛失又は該当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	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	可用性２の情報資産以外の情報資産	

(2)　情報資産の管理

① 管理責任

（ア）校内教育情報セキュリティ責任者は、情報資産について管理責任を有する。

（イ）校内教育情報セキュリティ責任者は、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、必要に応じてファイル(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)、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示するとともに､取扱制限についても明示する等適正な管理を行わなければならない。

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、該当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、該当情報を消去しなければならない。

④ 情報資産の入手

（ア）教職員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）教職員以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、該当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、入手した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、適正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、電磁的記録媒体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、該当電磁的記録媒体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、情報資産を適正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、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

（ウ）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、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。【推奨事項】

（エ）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、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿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

電子メール等により機密性２以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

⑧ 情報資産の提供

（ア）機密性２以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

（イ）機密性２以上の情報資産を外部に提供する者は、校内教育情報セキュリティ責任者に許可を得なければならない。

4　物理的セキュリティ

4-1　サーバ等の管理

⑴　機器の取付け

教育情報システム管理者は、サーバ等の機器の取付けを行う場合、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正に固定する等、必要な措置を講じなければならない。

⑵　機器の電源

① 教育情報システム管理者は、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、該当機器が適正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は、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。

⑶　通信ケーブル等の配線

① 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、施設管理担当課と連携し、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 教育情報セキュリティ管理者及び教育情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理担当課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 教育情報セキュリティ管理者及び教育情報システム管理者は、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正に管理しなければならない。

④ 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、教育委員会及び学校長から許可を得た又は契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

⑷　機器の廃棄等

教育情報システム管理者は、機器を廃棄、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。

4-2　通信回線及び通信回線装置の管理

① 校内教育情報セキュリティ責任者は、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、適正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正に保管しなければならない。

② 校内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に限定し、できる限り接続ポイントを減らさなければならない。

③ 校内教育情報セキュリティ責任者は、機密性２以上の情報資産を取り扱う教育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、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

④ 校内教育情報セキュリティ責任者は、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。

4-3　教職員の利用する端末や電磁的記録媒体等の管理

① 校内教育情報セキュリティ管理者は、盗難防止のため、必要に応じてモバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の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 校内教育情報セキュリティ管理者は、端末機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。【推奨事項】

5　人的セキュリティ

5-1　教職員の遵守事項

(1)　教職員の遵守事項

① 教育情報セキュリティポリシー等の遵守

教職員は、この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、速やかに校内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 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。

③ 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の外部における情報処理作業の制限

（ア）校内教育情報セキュリティ責任者は、機密性２以上、可用性２、完全性２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。

（イ）教職員は、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、校内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。

（ウ）教職員は、外部で情報処理業務を行う場合には、校内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 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

（ア）教職員は、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原則業務に利用してはならない。ただし、業務上必要な場合は、校内教育情報セキュリティ管理者の許可を得て利用することができる。

（イ）教職員は、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、校内教育情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

⑤ 持ち出し及び持ち込みの記録

校内教育情報セキュリティ管理者は、端末機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。

⑥ 机上の端末機等の管理

教職員は、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校内教育情報セキュリティ管理者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、適正な措置を講じなければならない。

⑦ 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。

⑧ 教育情報セキュリティポリシー等の掲示

校内教育情報セキュリティ責任者は、教職員が常に教育情報セキュリティポリシーを閲覧できるよう掲示しなければならない。

⑨ 委託事業者に対する説明

校内教育情報セキュリティ管理者は、ネットワーク及び教育情報システムの開発・保守等を委託事業者に発注する場合、委託事業者から再委託を受ける事業者も含めて、教育情報セキュリティポリシー等のうち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。

5-2　研修

(1)　情報セキュリティに関する研修

校内教育情報セキュリティ責任者は、定期的に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。

(2)　研修計画の策定及び実施

① 校内教育情報セキュリティ責任者は、教職員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。【推奨事項】

② 研修計画において、教職員は毎年度最低１回、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。【推奨事項】

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

(3)　研修への参加

全ての教職員は、定められた研修に参加しなければならない。【推奨事項】

5-3　情報セキュリティインシデントの報告

(1)　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、速やかに校内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 報告を受けた校内教育情報セキュリティ責任者は、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。

③ 校内教育情報セキュリティ責任者は、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及び教育情報統括管理責任者に報告しなければならない。

(2)　保護者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、保護者等外部から報告を受けた場合、校内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 報告を受けた校内教育情報セキュリティ責任者は、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。

③ 教育情報セキュリティ管理者は、該当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及び教育情報統括管理責任者に報告しなければならない。

④ 教育情報統括責任者は、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、保護者等外部から報告を受けるための窓口を設置し、該当窓口への連絡手段を公表しなければならない。【推奨事項】

(3)　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、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、教育情報統括管理責任者に報告しなければならない。

② 教育情報統括管理責任者は、教育情報統括責任者から、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。

5-4　ＩＤ及びパスワード等の管理

(1)　ＩＤの取扱い

教職員は、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。

(2)　パスワードの取扱い

教職員は、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（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）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、校内教育情報セキュリティ責任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。

⑤ 複数の教育情報システムを扱う教職員は、同一のパスワードを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 必要に応じて、仮のパスワード（初期パスワード含む。）は、最初のログイン時点で変更しなければならない。
⑦ 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。
⑧ 教職員間でパスワードを共有してはならない、ただし共用ＩＤに対するパスワードは除く。

6　技術的セキュリティ

6-1　コンピュータ及びネットワークの管理

(1)　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は、教職員が使用できる文書サーバの容量を設定し、教職員に周知しなければならない。
② 教育情報システム管理者は、教職員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については、標的型攻撃等によるファイルの外部流出を考慮し、ファイル暗号化等による安全管理措置を講じなければならない。

(2)　バックアップの実施

教育情報システム管理者は、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、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。

(3)　他団体との教育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は、他の団体と教育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及び教育情報統括責任者の許可を得なければならない。

(4)　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は、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 教育情報システム管理者は、教育情報システムにおいて、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正に管理しなければならない。
③ 教育情報システム管理者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委託事業者がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

(5)　情報システム仕様書等の管理

教育情報システム管理者は、ネットワーク構成図、システム仕様書について、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、適正に管理しなければならない。

(6)　ログの取得等

① 教育情報システム管理者は、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 教育情報システム管理者は、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、適正にログを管理しなければならない。
③ 教育情報システム管理者は、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。

(7) 障害記録

教育情報システム管理者は、教職員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、適正に保存しなければならない。

(8) ネットワークの接続制御、経路制御等

① 教育情報システム管理者は、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 教育情報システム管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

(9) 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は、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、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は、接続した外部ネットワークの瑕疵によりデータの漏えい、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、該当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 教育情報システム管理者は、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の判断に従い、速やかに該当外部ネットワークを物理的に遮断しなければならない。

(10) 複合機のセキュリティ管理

① 教育情報セキュリティ管理者は、複合機を調達する場合、該当複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件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は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③ 教育情報セキュリティ管理者は、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の全ての情報を抹消する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。

(11) 特定用途機器のセキュリティ管理

教育情報セキュリティ管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、該当機器の特性に応じた対策を講じなければならない。

(12) 無線ＬＡＮ及びネットワークの盗聴対策

① 教育情報システム管理者は、無線ＬＡＮの利用を認める場合、解読が困難な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 教育情報システム管理者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

(13) 電子メールのセキュリティ管理

① 教育情報システム管理者は、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 教育情報システム管理者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

③ 教育情報システム管理者は、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 教育情報システム管理者は、教職員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に周知しなければならない。

⑤ 教育情報システム管理者は、システム開発や運用、保守等のため教育委員会及び学校に駐在している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、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。

(14) 電子メールの利用制限

① 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。

② 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。

③ 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。

④ 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。

⑤ 教職員は、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。

(15) 無許可ソフトウェアの導入等の禁止

① 教職員は、端末機に無断でソフトウェアを導入してはならない。

② 教職員は、業務上の必要がある場合は、校内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、校内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、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。

(16) 機器構成の変更の制限

① 教職員は、端末機に対し機器の改造及び増設・交換を行ってはならない。

② 教職員は、業務上、端末機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、校内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の許可を得なければならな

(17) 無許可でのネットワークへの接続の禁止

教職員は、校内教育情報セキュリティ責任者の許可なく、端末機をネットワークに接続してはならない。

(18) 業務以外の目的でのウェブ閲覧の禁止

① 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。

② 校内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正な措置を求めなければならない。

(19)　無線ＬＡＮ及び移動体通信の利用制限

教職員は、校内教育情報セキュリティ責任者が認めた場合に限り、教育外部系（授業用）ネットワーク、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。

6-2　アクセス制御

(1)　アクセス制御等

① アクセス制御

校内教育情報セキュリティ責任者及び校内教育情報セキュリティ管理者は、ネットワーク又は教育情報システムごとにアクセスする権限のない教職員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。

② 利用者ＩＤの取扱い

（ア）校内教育情報セキュリティ責任者及び校内教育情報セキュリティ管理者は、利用者の登録、変更、抹消等の情報管理、教職員の異動、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。

（イ）教職員は、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、校内教育情報セキュリティ責任者又は校内教育情報セキュリティ管理者に通知しなければならない。

（ウ）校内教育情報セキュリティ責任者及び校内教育情報セキュリティ管理者は、利用されていないＩＤが放置されないよう、教育委員会と連携し、点検しなければならない。

③ 特権を付与されたＩＤの管理等

校内教育情報セキュリティ責任者及び校内教育情報セキュリティ管理者は、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、該当ＩＤのパスワードの漏えい等が発生しないよう、該当ＩＤ及びパスワードを厳重に管理しなければならない。

(2)　教職員による外部からのアクセス等の制限

① 教職員が外部から内部のネットワーク又は教育情報システムにアクセスする場合は、校内教育情報セキュリティ責任者及び校内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。

② 校内教育情報セキュリティ責任者及び校内教育情報セキュリティ管理者は、内部のネットワーク又は教育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 校内教育情報セキュリティ責任者及び校内教育情報セキュリティ管理者は、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 校内教育情報セキュリティ責任者及び校内教育情報セキュリティ管理者は、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 校内教育情報セキュリティ責任者及び校内教育情報セキュリティ管理者は、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 教職員は、持ち込んだ又は外部から持ち帰ったモバイル端末を校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、校内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。

⑦ 校内教育情報セキュリティ責任者及び校内教育情報セキュリティ管理者は、公衆通信回線（公衆無線ＬＡＮ等）を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。

(3) 認証情報の管理

① 校内教育情報セキュリティ責任者及び校内教育情報セキュリティ管理者は、教職員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。

② 教育情報統括責任者又は教育情報システム管理者は、認証情報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。

6-3 システム開発、導入、保守等

(1) 教育情報システムの調達

① 教育情報システム管理者は、教育情報システム開発、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 教育情報システム管理者は、機器及びソフトウェアの調達に当たっては、該当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。

(2) 教育情報システムの開発

システム開発における責任者及び作業者の特定

教育情報システム管理者は、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、システム開発のための規則を確立しなければならない。

(3) 教育情報システムの導入

① 教育情報システム管理者は、新たに教育情報システムを導入する場合、既に稼働している教育情報システムに接続する前に十分な試験を行わなければならない。

② 教育情報システム管理者は、個人情報及び機密性の高い生データを、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。

(4) 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正に整備・保管しなければならない。

(5) 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、他の教育情報システムとの整合性を確認しなければならない。

(6) 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。

6-4 不正プログラム対策

(1) 校内教育情報セキュリティ責任者の措置事項

校内教育情報セキュリティ責任者は、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、インターネットのゲートウェイにおいて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、インターネットのゲートウェイにおいて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の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 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
⑦ 業務で利用するソフトウェアは、原則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。また、該当製品の利用を予定している期間中に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する予定がないことを確認しなければならない。

(2) 教職員の遵守事項

教職員は、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 端末機において、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、該当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 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、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてＬＡＮケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

(3) 専門家の支援体制

教育情報統括責任者は、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。

6-5 不正アクセス対策

(1) 校内教育情報セキュリティ責任者の措置事項

校内教育情報セキュリティ責任者は、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を閉鎖しなければならない。
② 不要なサービスについて、機能を削除又は停止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正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。

(2) 攻撃への対処

校内教育情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、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、教育委員会と連絡を密にして情報の収集に努めなければならない。

(3) 記録の保存

校内教育情報セキュリティ責任者は、サーバ等に攻撃を受け、該当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、警察及び関係機関との緊密な連携に努めなければならない。

(4) 内部からの攻撃

教育情報統括責任者及び教育情報システム管理者は、教職員及び委託事業者が使用しているパソコン等の端末からの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。

(5) 教職員による不正アクセス

教育情報統括責任者及び教育情報システム管理者は、教職員による不正アクセスを発見した場合は、該当教職員が所属する校内教育情報セキュリティ責任者に通知し、適正な処置を求めなければならない。

(6) 標的型攻撃

教育情報統括責任者及び教育情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策(入口対策)や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策(内部対策及び出口対策)を講じなければならない。

6-6 セキュリティ情報の収集

(1) セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

教育情報統括責任者及び教育情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、該当セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

(2) 不正プログラム等のセキュリティ情報の収集・周知

教育情報統括責任者及び教育情報システム管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、教職員に周知しなければならない。

(3) 教育情報セキュリティに関する情報の収集及び共有

教育情報統括責任者及び教育情報システム管理者は、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。

7　運用

7-1　教育情報システムの監視

① 教育情報システム管理者は、セキュリティに関する事案を検知するため、教育情報システムを常時監視しなければならない。

② 教育情報システム管理者は、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。

③ 教育情報システム管理者が指名した者は、外部と常時接続するシステムを常時監視しなければならない。

7-2　教育情報セキュリティポリシーの遵守状況の確認

(1)　遵守状況の確認及び対処

① 教育情報統括責任者及び教育情報システム管理者は、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、速やかに教育情報統括管理責任者に報告し、適切に対処しなければならない。

② 教育情報統括責任者及び教育情報システム管理者は、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正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及び教育情報システム管理者が指名した者は、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等の利用状況を調査することができる。

(3)　教職員の報告義務

① 教職員は、このポリシーに対する違反行為を発見した場合、直ちに校内教育情報セキュリティ責任者及び校内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 該当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が判断した場合において、教職員は、緊急時対応計画に従って適正に対処しなければならない。

7-3　侵害時の対応

(1)　緊急時対応計画の策定

教育情報統括責任者は、情報セキュリティインシデント、教育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正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には該当計画に従って適正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・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、該当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。

(4)　緊急時対応計画の見直し

教育情報統括責任者は、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。

7-4　例外措置

(1)　例外措置の許可

教育情報統括責任者及び教育情報システム管理者は、情報セキュリティ関係規定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する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の許可を得て、例外措置を講じることができる。

(2)　緊急時の例外措置

教育情報統括責任者及び教育情報システム管理者は、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に報告しなければならない。

(3)　例外措置の申請書の管理

教育情報統括責任者及び教育情報システム管理者は、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

7-5　法令遵守

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に、次の法令のほか関係法令を遵守し、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 サイバーセキュリティー基本法(平成12年法律第104号)
⑦ 池田市個人情報の保護に関する法律施行条例（令和4年条例第24号）

7-6　懲戒処分等

(1)　懲戒処分

教育情報統括責任者は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、該当教職員が所属する校内教育情報セキュリティ責任者に通知し、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。

(2)　違反時の対応

該当教職員は違反の重要性、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。

8　業務委託と外部サービスの利用

8-1　業務委託

(1)　委託事業者の選定基準

① 教育情報システム管理者は、委託事業者の選定にあたり、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、委託事業者を選定しなければならない。【推奨事項】

(2)　契約項目

重要な情報資産を取扱う業務を委託する場合には、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の遵守
・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・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委託事業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
・市による監査、検査
・市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)

(3)　確認・措置等

教育情報システム管理者は、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、(2)の契約に基づき措置を実施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に報告しなければならない。

8-2　約款による外部サービスの利用

(1)　約款外部サービスの利用に係る規定の整備

教育情報システム管理者は、以下を含む外部サービスの利用に関する規定を整備すること。また、該当サービスの利用において、機密性の高い情報が取り扱われないように規定しなければならない。

① 約款によるサービスを利用してよい範囲
② 業務により利用する約款による外部サービス
③ 利用手続及び運用手順

(2)　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。

9　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。

(1)　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。

(2)　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、無断提供しないこと。

(3)　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

学校、教育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。

(4)　不必要な個人プロファイル作成の禁止

学校､教育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保護された場合を除き、不必要な個人プロファイルを作成しないこと。

(5)　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。

(6)　個人情報の保持期間の定義

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

(7)　個人情報の利用目的

個人情報を収集、使用、共用及び保持するのは、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。

(8)　個人情報の取り扱いについての情報開示

個人情報の取り扱いについて、契約又はプライバシーポリシーで明確に示すこと。

(9)　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。

(10)　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、漏えい、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、個人情報を正確にかつ最新の状態で管理すること。

(11)　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、個人情報保護法等を遵守し、該当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。

(12)　合併・買収

合併又は他社による買収を行う場合、後継企業が以前に収集してい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。

10　点検・評価・見直し

(1)　実施方法

教育情報統括責任者及び教育情報システム管理者は、教育情報システム及び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、毎年度及び必要に応じて点検を行わなければならない。また、委託事業者に委託している場合、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、定期的又は必要に応じて点検を行わなければならない。

(2)　報告

教育情報統括責任者及び教育情報システム管理者は、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に報告する。

(3)　保管

教育情報統括責任者及び教育情報システム管理者は、点検の実施を通して収集した点検結果、点検報告書の作成のための調書等を、紛失等が発生しないように適正に保管しなければならない。

(4)　点検結果への対応

教育情報統括責任者及び教育情報システム管理者は、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に報告し対処しなければならない。

(5)　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等への活用

教育情報統括責任者及び教育情報システム管理者は、情報セキュリティ自己点検の結果及び情報セキュリティに関する状況の変化等を踏まえ、このポリシー及び関係規程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場合、改善を行うものとする。

11　生成ＡＩの利用について

生成ＡＩは、業務効率の改善や新しいアイディア出しなどに役立つ反面、入力したデータがバックグラウンドで学習され、第三者の回答に利用される可能性があるなど、情報が他に漏洩・拡散するリスクがある。また、入力するデータの内容や生成物の利用方法によっては法令に違反したり、他者の権利を侵害したりする可能性がある。「初等中等教育段階における生成ＡＩの利活用に関するガイドライン（Ｖｅｒ．２．０）（文部科学省初等中等教育局令和６年１２月２６日公表）」（https://www.mext.go.jp/a_menu/other/mext_02412.html）を参照し、適切に生成ＡＩを利用すること。

池田市立学校教育情報セキュリティポリシー
令和８年３月発行
池田市教育委員会