第１章 情報セキュリティ基本方針

１．目的

現在、愛川町立小学校及び中学校（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、高速大容量の通信ネットワークの整備、一人一台の端末等ＩＣＴ環境の整備を行い、個別に最適化された教育環境の実現を推進している。

学校が取り扱う情報には、児童生徒（以下「児童生徒等」という。）、保護者、教職員等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、学校でのＩＣＴ利用にあたって、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。

令和４年４月に本セキュリティポリシーを策定したところであるが、文部科学省「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、本セキュリティポリシーを改定するもとする。

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る。このポリシーは、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の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 。

文　書	内　容	
愛川町教育委員会 教育情報セキュリティポリシー	情報セキュリティ基本方針	学校のセキュリティ対策の目的や原則を定めた統一的な規範
	情報セキュリティ対策基準	学校にある情報を脅威から守るための具体的な対策を示したもの

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。

（１）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。

（２）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。

（３）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。

（４）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。

（５）学校情報

電磁的に記録された学校事務の執行に関わる情報をいう。

（６）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（ハードウエア及びソフトウエア）をいい、校内においては以下のとおり分類する。

分類	内容	役割と利用環境
①校務系ネットワーク	教職員が、機密性・完全性の高い学校情報（指導要録、人事情報、成績情報等）を取り扱う校務処理に用いる情報システム及びネットワーク。	校務系情報を取り扱うことを目的とし、外部からのアクセスを厳格に制限するか、学習系とは論理的又は物理的に分離するものとする。インターネット接続する場合は、限定的な通信先に限り、厳格な制御を施す。
②学習系ネットワーク	児童生徒及び教職員が、学習活動、授業支援に用いるコンピュータ、１人１台端末等、教育活動全般に用いる情報システム及びネットワーク。	児童生徒の学習用端末や、教育委員会が許可したクラウドサービス（学習ツール等）への接続に利用する。情報セキュリティ対策基準に基づき、フィルタリングや不正プログラム対策を講じるものとする。

（７）情報資産の重要性分類

情報資産の機密性、完全性、可用性の観点から、侵害された場合の被害の程度に基づき、以下の４段階に分類する。

ア．重要性分類 Ⅰ：情報が侵害された場合に甚大な被害が想定され、学校もしくは特定個人が著しい不利益を被る情報。（指導要録原本等）

イ．重要性分類 Ⅱ：情報が侵害された場合に大きな被害が想定され、学校もしくは特定個人が大きな不利益を被る情報。（通知表、採点結果、進路希望調査等）

ウ．重要性分類 Ⅲ：情報が侵害された場合に学校もしくは特定個人が不利益を被る情報。（出席簿、学習記録等）

エ．重要性分類 Ⅳ：上記以外で、セキュリティ侵害が発生してもほとんど影響を及ぼさない情報。（学校要覧、ウェブ掲載情報等）

（８）サーバ等

ネットワーク上で学校情報を処理し、端末機に提供するコンピュータをいう。

（９）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をいう。

(10) 情報システム

学校情報を処理するためのハードウエア及びソフトウエアをいう。

(11) 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）をいう。

ハードディスク、ＵＳＢメモリ等。

(12) 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型端末など、携行可能な多機能端末をいう。

４．情報資産への脅威

情報資産に対して想定される脅威は、その発生度合や発生した場合の影響を考慮するものとし、次のとおりとする。

（１）部外者による意図的な不正アクセス、又は不正操作によるデータやプログラムの漏えい・持出・盗聴・改ざん・消去、機器及び記録媒体の盗難等

（２）教職員等及び外部委託業者による非意図的な操作、又は意図的な不正アクセス又は不正操作によるデータやプログラムの漏えい・持出・盗聴・改ざん・消去、機器及び記録媒体の盗難、規定外の情報システム接続や操作によるデータ漏えい等

（３）地震、落雷、火災、水害等の災害並びに事故、故障等による業務の停止

５．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、次に定める情報セキュリティ対策を講ずるものとする。

（１）管理体制

情報資産を管理し、機密性、完全性および可用性を維持するための体制を確立する。

（２）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。

（３）人的セキュリティ対策

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、全ての教職員等にこのポリシーを周知徹底するための教育を実施する等、必要な対策を講ずる。

（４）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、コンピュータウイルス対策ソフト導入等の技術面における対策を講ずる。

（５）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．情報セキュリティポリシーの適用範囲

このポリシーの適用範囲は、学校が保有する全ての情報資産を取り扱う以下のシステム等とする。

（１）学校、教育委員会における学校用の情報システム及びサーバ。

（２）教育委員会が利用を許可し、導入したクラウドサービス。

（３）教職員及び児童生徒に貸与された端末（スマートデバイスを含む。）を通じた、校務系・学習系の情報資産の利用全て。

７．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、及び教育委員会に所属する職員（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、このポリシーを遵守しなければならない。

８．監査及び自己点検

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。

９．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。