和光市立小・中学校教育情報セキュリティ基本方針

和光市立小・中学校教育情報セキュリティ基本方針

和光市教育委員会

１　趣旨

学校の各情報システムが取り扱う情報には、個人情報のみならず行政や学校の運営上重要な情報など、部外に漏洩等した場合には極めて重大な結果をもたらす情報が多数含まれている。

したがって、これらの情報資産及び情報を取り扱うネットワーク及び情報システムを内部、外部からの様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、教育活動や事務の継続的かつ安定的な運営のためにも必要不可欠である。ひいては、このことが学校に対する市民からの信頼の維持向上にも寄与するものである。

そのため、学校が保有する情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を整備することを目的として教育情報セキュリティポリシーを策定し、教育情報セキュリティ基本方針については学校の情報セキュリティ対策の基本的な方針として、教育情報セキュリティポリシーの対象、位置付け等を定めるものとする。

２　用語の定義

⑴　ネットワーク

学校のコンピュータを相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

⑵　教育情報システム

本市の学校教育において使用されるコンピュータやネットワーク、及び電磁的記録媒体等で構成され、情報処理を行う仕組みをいう。

⑶　情報資産

ネットワーク及び教育情報システムで取り扱うすべての電磁的に記録されたデータ及びこれらを印刷した文書を含めた全ての情報をいう。

⑷　情報セキュリティ

情報資産の機密の保持、正確性及び完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

⑸　機密性(confidentiality)

情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

⑹　完全性(integrity)

情報および処理の方法の正確さおよび完全である状態を安全防護すること。

⑺　可用性(availability)

許可された利用者が必要なときに情報にアクセスできることを確実にすること。

３　教育情報セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務

教育情報セキュリティポリシーは、教育委員会及び学校が保有する情報資産に関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、情報セキュリティ対策の頂点に位置するものである。

したがって、学校に関わるすべての職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識をもつとともに業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

4 情報セキュリティ管理体制

学校の情報資産について、職員等及び外部委託事業者がそれぞれの責任において率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

5 情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

6 情報資産への脅威

教育情報セキュリティポリシーを策定するうえで、情報資産に対する脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は次に掲げるとおりである。

⑴ 部外者の侵入、盗難及び故意の不正アクセス又は不正操作による機器もしくは情報資産の持ち出し、破壊、盗聴、改ざん、消去等

⑵ 職員等又は外部委託事業者による意図しない操作及びアクセスのための認証情報もしくはパスワードの不適切管理、故意の不正アクセス又は不正操作による情報資産の持ち出し、破壊、盗聴、改ざん、消去並びに機器及び記録媒体の盗難及び規定外の情報システムの機器操作並びに規定外の端末接続によるデータ漏洩等

⑶ コンピュータウィルス、地震、落雷、火災等の災害や事故、故障等によるサービス及び業務の停止

7 情報セキュリティ対策

情報資産を前項の脅威から保護するため、次に掲げる情報セキュリティ対策を講じるものとする。

⑴ 人的セキュリティ対策

情報セキュリティに関する権限及び責任並びに遵守すべき事項を定め、職員等に対する周知徹底を図るとともに、十分な教育及び啓発が行われるよう必要な対策を講じる。

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並びに情報資産への損傷及び妨害等から保護するための物理的な対策を講じる。

⑶ 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、ネットワーク管理等の技術的対策を講じる。

⑷ 運用等におけるセキュリティ対策

ネットワークの監視、情報セキュリティ対策の遵守状況の確認等、運用面の対策を講じる。また、緊急事態が発生した際に迅速かつ適切な対応を可能とするための危機管理対策を講じる。

8 教育情報セキュリティ対策基準の策定

学校の情報資産について、適切に情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した教育情報セキュリティ対策基準を策定するものとする。

9 教育情報セキュリティ実施手順の策定

教育情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対

する脅威及び情報資産の重要度に対応する教育情報セキュリティ対策基準の基本的な要件に基づき、情報資産の情報セキュリティ実施手順を策定するものとする。

10　情報資産の分類

情報資産をその重要度に応じて分類し、それに応じた情報セキュリティ対策を行うものとする。

11　対策基準及び実施手順の扱い

対策基準及び実施手順は、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であることから非公開とする。

12　職員等及び外部委託事業者の義務

職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たっては、情報セキュリティに関係する法令等及び情報セキュリティポリシーを遵守する義務を負うものとする。

13　情報セキュリティに関する違反への対応

情報セキュリティポリシーに違反した者については、その重大性、発生した事案の状況等に応じて懲戒処分等の対象とする。

14　情報セキュリティ監査の実施

情報セキュリティ対策が遵守されていることを検証するため、定期的に監査を実施するものとする。

15　評価及び見直しの実施

情報セキュリティ監査の結果等により、教育情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報システムの変更、情報セキュリティを取り巻く状況の変化を踏まえ、教育情報セキュリティポリシー及び実施手順の見直しを適宜実施するものとする。

附　則

この教育情報セキュリティ基本方針は、令和７年４月１日から施行する。