北名古屋市教育委員会
情報セキュリティ基本方針

北名古屋市教育委員会

1　目的

学校では、児童生徒に対する教育活動の充実と校務の効率化を目的に情報化を積極的に推進している。一方、学校で取り扱う情報には、児童生徒及び保護者、教職員、その他地域住民等の個人情報等万一外部に漏えい等した場合には極めて重大な結果を招く重要な情報が多数含まれている。

したがって、学校の情報化の推進に当たっては、情報漏えい、改ざん、紛失等の脅威から情報資産を防御することが必要不可欠であり、児童生徒、保護者、地域住民等の財産、プライバシー等を守ることが信頼される学校づくりにも寄与するものである。

そのため、学校の情報資産の情報セキュリティ対策を整備するために北名古屋市教育委員会情報セキュリティポリシー（以下、「情報セキュリティポリシー」という。）を定めることとし、このうち、情報セキュリティ基本方針については、当市学校の情報セキュリティポリシー対策の基本的な方針として、情報セキュリティの対象、位置付け等を定めるものとする。

2　定義

⑴　ネットワーク

コンピューター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。

⑵　情報システム

コンピューター、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

⑶　情報資産

ネットワーク及び情報システムの開発と運用に係るすべての情報並びにネットワーク及び情報システムで取り扱うすべての情報をいう。

なお、情報資産には、紙等の有体物に記録された情報を含むものとする。

⑷　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。

⑸　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障害・事故及びシステム上の欠陥をいう。

3　教職員等及び外部委託事業者の情報セキュリティポリシー遵守義務

情報セキュリティポリシーは、学校が保有、管理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と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、学校の情報資産に関する業務に携わるすべての教職員等及び外部委託事業者は、情報セキュリティの教職員等を認識すると共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、教育委員会及び当市学校の管理職が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。

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　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。

⑴　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

⑵　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、外部委託管理の不備、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

⑶　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

７　情報セキュリティ対策

上記６で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずる。

⑴　物理的セキュリティ

サーバー等、情報システム室等、通信回線等及び教職員等のパソコン及びタブレット等のモバイル端末（以下「パソコン等」という。）の管理について、物理的な対策を講ずる。

⑵　人的セキュリティ

情報セキュリティに関し、教職員等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ずる。

⑶　技術的セキュリティ

コンピューター等の管理、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ずる。

⑷　運用

情報システムの監視、情報セキュリティ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、情報セキュリティポリシーの運用面の対策を講ずる。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

等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

⑸　外部委託とクラウドサービスの利用

ア　外部委託を行う場合には、外部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する。また、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確認し、必要に応じて契約に基づき措置を講ずる。

イ　クラウドサービスを利用する場合には、確認すべきセキュリティ項目及びクラウド利用者側の管理方針・体制についての規定を整備し、対策を講ずる。

ウ　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

情報セキュリティポリシーの遵守状況を検証するため、定期的また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　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び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、情報セキュリティポリシーを見直す。

10　情報セキュリティ対策基準の策定

上記７、８及び９に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

11　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定する。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情報セキュリティ対策基準の基本的な要件に基づき、教育委員会及び学校単位で情報資産の情報セキュリティ実施手順を策定する。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより学校運営に重大な支障を及ぼす恐れがあることから非公開とする。