学校情報セキュリティ

１ 情報セキュリティの基本方針

児童（生徒)、保護者、教職員などの個人情報及び学校運営上の重要な教育情報を保護して適切に管理・運用するためのルールを定める。

２ 組織・体制

(1) 校長は、すべての情報セキュリティに関する権限及び責任を負う。
(2) 職員は、本情報セキュリティポリシーの内容を遵守しなければならない。
(3) 校務分掌に情報セキュリティ担当者(教頭等)を置く。
(4) 職員は、校内において知り得た情報をいかなる場合も学校外で漏らしてはならない。
(5) 新任者には、情報セキュリティの研修会を行う。
(6) システムで使用するパスワードは、他人に推測されにくいものとし、その管理は十分に行う。

３ 情報機器・ネットワーク管理

(1) 情報セキュリティ担当者は、コンピュータ室並びにセキュリティ USB キー（以下、「A-Locky」）を利用してサーバ内のフォルダの管理を行う。また USB メモリや CD-R、FD 等の入力記憶媒体（以下、記憶媒体）を使用させてもよいが、それらの記憶媒体は、全て施錠し保管する。使用時は、校長の許可を得るものとする。

なお、サーバ内のフォルダには、次のものがある。

・共通フォルダ
「A-Locky」を利用して教職員全員が接続できるフォルダ
児童生徒名簿等の担当教職員が使う個人情報ファイル､教職員が共通に使うファイルを保存しておく

・個人フォルダ
「A-Locky」を利用して接続できる個人用フォルダ
教職員のみが使う個人情報ファイルを保存しておく

・その他フォルダ（小学校は「先生専用」フォルダ、中学校は「校務フォルダ」）
「A-Locky」を利用しなくても接続できる個人用フォルダ
児童・生徒の写真や個人情報を含まないデータなどを保存しておく

(2) 情報セキュリティ担当者は、学期末や学年末に共通フォルダの保存データの整理・削除を行い、個人フォルダの保存データの整理・削除を指導する。特に、長期保存が必要なものを除き、転出児童・生徒や卒業生のデータ等の削除を忘れずに行う。

(3) 公的なパソコンをネットワークに接続する際、情報セキュリティ担当者が次の条件がすべて整っているかどうかを点検した結果を勘案して、校長の許可を得る。

次のＯＳ（基本ソフト）が入っており、最新のサービスパックとウイルス対策ソフトがインストールされていること。(Windows 7、 Vista、XP、2000)

② 最新の Windows Update を、定期的に更新（自動更新）していること。

③ ウイルス対策ソフトを導入し、そのパターンファイルを常に最新のものにしていること。

④ 自動的に、毎日ウイルス対策ソフトを起動するように設定していること。

(4)上記(3)の事項を確認するために、定期的な資産管理サービス（以下、「PCScan」）を準備しているので、そのサービスの利用も行うこと。

(5) 情報セキュリティ担当者は、ネットワークに接続している公的なパソコンを定期的にウイルスチェックをして、ウイルスが発見された場合「クリーンナップ」等、適切に処置するように指導する。

(6)個人所有のパソコンをネットワークに接続してはならない。

(7) ネットワークに接続して使用するパソコンにソフトウェアをインストールする場合やメモリ等を増設する場合は、校長・教育委員会の許可を得ること。

(8) 電子メール添付ファイルは必ずウイルスチェックを行う。

(9)校長より許可を得て USB メモリ(含 UMCrypt)を使用する際には、事前に必ずウィルスチェックを行うこと。

(10) ネットワークシステム等を勝手に改変してはならない。

(11) 不正アクセス等を防止するため、情報システムを利用するすべての者は、適切なパスワードの管理を行わなければならない。

(12) インターネットの利用や電子メールの利用については、職務に関することに限定する。

４　個人情報の保護

(1) 個人情報に関するデータは学校フォルダにのみ保存する。パソコンや記憶媒体に保存してはならない。

(2) 児童（生徒）に関する指導記録、名簿、成績などのデータをコピー又は印刷して、校外へ持ち出さない。やむを得ず持ち出す場合は、校長の許可を得た後、デジタルデータに関してはセキュリティ USB メモリ（以下、「UMCrypt」）を利用すること。

(3)校外に持ち出している間は、UMCrypt 内に保存し、必ず学校サーバに戻し、UMCrypt には個人情報のデータを削除した後、校長に報告する。

(4)なお校外のパソコンで UMCrypt を利用する際は、必ずウイルス対策ソフトを導入し、そのパターンファイルを常に最新のものにすること。

５ その他利用規程

(1) サーバの利用が終了した際には、適切な手順に従ってフォルダへの接続を切断する。
(2) 席を離れる場合は、キーロック等の不正アクセス防止のために適切な処置を講ずる。
(3) インターネット等を利用する際は、個人情報、肖像権、著作権を侵害しない。
(4) ＩＤ、パスワードは適切に管理する。
(5) インターネット等を利用する際は、インターネット・モラル（ネチケット）を心がける。
(6) 使用アプリケーション類（Word、Excel、一太郎等）は、セキュリティホールが改善された最新版に更新する。
(7) 「A-Locky」、「UMCrypt」の本格稼働後は記憶媒体を基本的には使用しない。

６ 運用

(1) 校長及び情報セキュリティ担当者は、本ポリシーが適切に遵守されているか確認する。また、重大なポリシー違反が明らかになった場合は、(2)に示す対応を迅速に行う。
(2) 緊急時の対応については、校長に報告する。校長は、速やかに教育委員会に報告する。また、情報セキュリティ担当者は、原因の特定、被害や影響の範囲の把握、経過の記録などを行い、被害が拡大しないようネットワークを停止し、ヘルプデスクへ連絡するなどの対応を行う。

７ 評価・監査・見直し

校長は、常に本ポリシーの実態との相違等を評価し監査を行う。また、その結果、必要な場合は見直し及び更新を行う。