甲府市立北新小学校情報セキュリティポリシー

1 情報セキュリティの基本方針

教育公務員として守秘義務の徹底を図る一環として，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 対象者

情報セキュリティポリシーの対象は、本校の職員とする。

3 組織・体制

(1) 学校長は、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を置く。
(4) 職員は、本校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) 職員は、学校ネットワーク内での不正アクセスをしてはならない。
(6) 新任者には、本校に赴任した日から１週間以内に情報セキュリティの研修会を行う。
(7) 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。

4 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グループセッションを経由した個人情報管理用センターサーバ内の本校用のフォルダ（以下、学校フォルダ）の管理を行う。
なお、学校フォルダには、次のものがある。
・重要情報保管フォルダ（グループセッションを経由して接続できる学校インターネット内のフォルダで、児童生徒名簿等の担当教職員が使う個人情報ファイルを保存しておく）
・共有フォルダ（グループセッションを経由して接続できる学校インターネット内のフォルダで、教職員全員が接続でき、教職員が共通に使う個人情報以外のファイルを保存しておく）
・個人用フォルダ（職員室からのみ接続できる学校インターネット内の個人用フォルダで、成績ファイル等の当該教職員のみが使う個人情報ファイルを保存しておく）
(2) 情報セキュリティ担当者は、学期末や学年末に重要情報保管フォルダの保存データの整理・削除を行い、学年フォルダや個人用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、記帳し学校長の許可を得る。
① 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ィルス対策ソフトがインストールされていること。
・Windows 8
・Windows 7
・Windows Vista
② 最新の Windows Update を、定期的に更新（自動更新）していること。
③ ウィ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、毎日ウィルス対策ソフトを起動するように設定していること。
(4) 校内でネットワークに接続せずに公的なパソコンや個人のパソコンを使用する際、情報セキュリティ担当者は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、記帳し学校長の許可を得る。
・ (3)の①に該当し、コンピュータウィルスに感染していないことが確認できたもの。
・ 上記機種でない場合、 旧ＯＳ（Windows 2000, Windows Me、Windows 98〔含むSE〕、Windows 95）の機種で、コンピュータウィルスに感染していないことが確認できたもの。
(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ィルスチェックをして、ウィ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) 基本的に個人のパソコンをネットワークに接続してはならない。特殊な事情が生じてある期間接続する必要が生じた場合は、記帳し学校長の許可を得るものとする。ただし、その場合も期限を区切って許可を出し、長期間にわたり接続しないものとする。
(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、記帳し学校長の許可を得る。
(8) 電子メール添付ファイルは必ずウィルスチェックを行う。
(9) ネットワークシステム等を勝手に改変してはならない。
(10) 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。
(11) インターネットの利用や電子メールの利用については、職務に限定する。

5 個人情報の保護

(1) 学校及び自宅において、校務や児童（生徒）の個人情報を扱うパソコンにはファイル交換ソフトをインストールしない。

(2) 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。
（※ 「個人情報に関するデータ」の定義に関しては、別紙「個人情報の定義について」を参照）

(3) 児童（生徒）に関する指導記録、名簿、成績などの原本、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、学校長の許可を得た後、個人情報校外持ち出し申請書に記入する。デジタルデータに関してはグループセッションを経由した個人用フォルダを利用する。その際、個人用フォルダからデータをダウンロードしてはならない。直接、フォルダ内のデータを操作する。ただし、家庭で常時接続のブロードバンド等でインターネットを利用できない教職員については、記帳し学校長の許可を得て、ＩＤやパスワードで守られたＵＳＢメモリ等を利用することは可能であるが、家庭に持ち帰る日と次の日のみＵＳＢメモリ内に保存し、次の日には学校フォルダに戻し、ＵＳＢメモリには個人情報のデータを削除した後、学校長に報告する。

(4) 個人情報の管理に関して、(2)のとおり、パソコンや記憶媒体に保存してはならないが、センターサーバ導入前に保存した後削除したパソコンや記憶媒体を廃棄する際は、パソコンのハードディスクや記憶媒体の全体を物理フォーマットする。廃棄を業者に委託する場合は、個人情報を完全に削除し漏洩しないような契約を結ぶ。

(5)その他の個人情報の管理については，別紙２「その他の個人情報管理マニュアル」を参照

6 その他の教職員用利用規程

(1) 成績処理等、個人情報のデータは学校フォルダにのみ保存する。

(2) 学校フォルダのデータを利用する際には、パソコンや記憶媒体にダウンロードせず、直接操作する。その際、不用意な操作ミスに備えて、学校フォルダ内にバックアップしておく。ただし、使用ソフトの特性上、ファイルをダウンロードしなければデータ処理ができない場合のみ、記帳し学校長の許可を得た後、一時的にダウンロードし、データ処理後は必ず学校フォルダに戻しておく。

(3) 学校フォルダ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。

(4) 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。

(5) 教育情報を電子メールで送付する場合、重要度に応じてセキュリティ対策を講ずる。

(6) 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）を心がけると共に，個人情報、肖像権、著作権を侵害しない。

(7) ＩＤ、パスワードは適切に管理する。

(8) 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。

(9) 個人情報のデータは記憶媒体を基本的には使用しない。個人情報以外のデータは４の(3)または(4)に対応し、更に記憶媒体自体にもウィルスチェックを行って問題がなく、そのことを記帳し学校長に報告し許可を得た場合のみ使用することができる。

その際、次のような対応をすること。

① ４の(3)に該当する機種から取り外し、他の４の(3)に該当する機種に取り付ける場合は、両方のパソコンのウィルス対策ソフトで、ウィルス・スキャンを行う。

② ４の(3)に該当する機種から取り外し、他の４の(4)に該当する機種に取り付ける場合は、４の(3)のパソコンのウィルス対策ソフトで、ウィルス・スキャンを行って取り外す。

③ ４の(4)に該当する機種から、４の(3)に該当する機種には、できる限り接続しない。やむを得ず、接続する場合は、接続と同時にウィルス・スキャンを行ってからファイルを開く。

④ 外部記憶媒体を取り付けたときに、ファイルが自動起動しないよう設定しておく。

7 運用

(1) 学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学期 1 回(最初の職員会議)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、学校長に報告する。学校長は、速やかに甲府市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。

8 評価・監査・見直し

学校長は、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。

附則　平成 26 年 1 月　改訂