韮崎市立韮崎北東小学校情報セキュリティポリシー

韮崎市立韮崎北東小学校

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　対象者

　情報セキュリティポリシーの対象者は，本校の職員とする。

３　情報セキュリティポリシーとは

　「情報資産」を守るために施す対策や規約をまとめたものを**「情報セキュリティポリシー」**と呼ぶ。

　これまで「セキュリティ」というとネットワークセキュリティの技術的な側面だけでなく，物的，人的なセキュリティまで考慮する必要がある。
　わたしたちが守るべき「情報資産」は必ずしも電子的なものばかりではなく，情報を印刷した文書，メモ、人が話す内容など，さまざまな形態がある。

４　組織・態勢

（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）校務分掌において情報セキュリティ担当者を置く。
（４）職員は，異動・退職などの場合には，知り得た情報を学校外では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。

５　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職員用センターサーバの学校用フォルダの管理を適切に行う。
（２）情報セキュリティ担当者は，学期末や学年末に学校用フォルダの保存データの整理・保存を行う。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個人データ等の削除を必ず行う。
（３）個人のパソコンは，持ち込み禁止。ネットワークや LAN にも接続しない。
（４）使用するパソコンに，ソフトウエアを許可なくインストールすることを禁止する。
（５）校務処理を行う機器には，ウィルス対策ソフトをインストールし，常に新しいパターンファイルをダウンロードし，最新の状況にしておく。
（６）電子メール添付ファイルは，ウィルスチェックを行う。迷惑メール，営業メールは，即時削除する。

（７）ネットワークシステムを勝手に改変しない。
（８）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。
（９）職員室のパソコンを起動させるためには，機種ごとにＩＤとパスワードが一致するように設定する。そのＩＤとパスワードは，外部のものには，容易には推測されないように情報担当が管理する。
（10）インターネットや電子メールの利用は，職務に限定する。

６　個人情報の保護

（１）校務や児童の個人情報を扱うパソコンには，ファイル交換ソフト（ウイニーなど）をインストールしない。
（２）児童生徒に関する指導記録，名簿，成績などのデータ，そのコピー，または印刷したものを絶対に校外に持ち出さない。補助資料等をやむを得ずに持ち出す場合には，学校長の許可を得る。
（３）個人情報を保存した後，削除したＵＳＢメモリやＣＤ等の入力記憶媒体やパソコンを廃棄する場合は，入力記憶媒体やパソコンのハードディスク全体をフォーマットする。
（４）個人情報の持ち出しに関して，原則として校外への持ち出しを禁じる。特に指導要録，通信表，健康カードは，校外への持ち出しは禁止する。
（５）電話番号や住所，成績補助簿等をやむを得ず校外に持ち出さなければならない場合は，管理職の許可を得て，「個人情報等校外持ち出し許可簿」に記入する。
（６）個人情報に関する職員の意識が適切に保たれるよう，学校長をはじめ，情報担当が機会あるごとに注意を喚起して，意識を高く保つように指導する。
（７）管理職は，毎朝，「個人情報等校外持ち出し許可簿」を点検する。
（８）教頭，または情報セキュリティ担当者は，退勤する前に校外への持ち出しが禁止されている公簿，及びＵＳＢなどの記憶媒体の保管が適切になされているか点検する。

７　その他の教職員用利用規程

（１）成績処理等，個人情報に関するデータは，学校のパソコンに保存し，他には保存しない。
（２）席を離れる場合は，キーロック，シャットダウン等の不正アクセス防止のために適切な処置を講じて，席を立つこと。
（３）個人情報，教育情報等は，電子メールで送信しない。
（４）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。
（５）ＩＤ，パスワードは，適切に管理する。（忘れない，教えない，推測されない）
（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。
（７）個人情報をＵＳＢ等には保存しない。ＵＳＢメモリー等の記憶媒体を用いてファイルを開くときは，暗証番号などをかけ，（万が一紛失してしまった場合にも）他者からすぐに開けないようにする。また，名簿など重要な情報，文書についても暗証番号をかけセキュリティを確保する。
（８）退勤時にはパソコンをシャットダウンする。（雷の季節【５月～９月】には，電源コード，

ＬＡＮコードを抜いてから退勤する。最寄りで気を遣い，声をかけ合う。サーバーの電源を切る。）

（９）異動または職場の配置換えでパソコンが変わる場合、使用していたパソコンのハードディスク内を整理し、初期設定の状態にして渡すようにする。

（10）電話連絡網，家庭環境調査票，住所録，メールアドレスなどの個人情報は，職員室内で管理・保管する。原則として職員室外への持ち出しを禁止する。

（11）各学年で，個人情報の持ち出しが無いように，学年主任を中心に声かけをする。学年用ＵＳＢは，必ず耐火金庫に保管する。

（12）机上パソコンの職員室外への持ち出しは，原則として禁止している。

（13）電子黒板等の関係で，机上パソコンを教室等で使用する場合は，机上パソコンではなく，電子黒板用のパソコンを割り当てて使用する。机上パソコンを教室等で使用する場合は，情報担当にその旨を申し出て，適切に使用する。

８　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，随時確認する。また，重大なポリシー違反が明らかになった場合は（２）に示すよう迅速に行う。

（２）情報事故の場合は，まず，学校長に連絡する。学校長は速やかに教育委員会に連絡する。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にネットワークを停止したり，関係機関へ連絡したりするなどの対応を迅速に行う。

９　評価・監査・見直し

学校長は，本ポリシーと実態との相違等を常に評価し監査を行う。また，その結果必要な場合は，見直し及び，更新を行い，変更点の周知と徹底を行う。