五加小学校　情報セキュリティポリシー

１　目的

五加小学校の情報資産を守るため，情報セキュリテイに関する基本的事項を定める。

２　対象範囲と対象情報資産

①　情報セキュリティポリシーの対象範囲は，五加小学校の情報資産を利用する全員である。

②　機密情報資産とは，指導要録，通知票，児童名簿，家庭環境調査票などであり，及び，それらを保存する媒体（CD,　USB メモリ等）である。(「情報資産一覧表参照」)

３　管理体制

①　学校長が中心となり，情報セキュリティ対策をする。

４　情報資産の取扱い

①　原則として複製及び校外への持ち出しはしない。持ち出す必要がある場合は，「情報資産持ち出し許可申請書」を提出して，校長の許可を得る。

②　校外へ発信する情報については，校長の許可を得ること。

③　個人情報を収集する場合は，目的・管理方法等を明らかにして，校長の許可を得る。

④　電話等の問い合わせには，原則として個人情報を提供しない。

⑤　情報資産は保存期間を明記し，適正に保存する。保存期間が終了したものは，適正な方法で廃棄する。

５ 電子媒体等による情報セキュリティ対策

(1) 人的セキュリティ対策

①　コンピュータの利用は，情報の破損等がないよう，各自が責任を持って管理する。

②　コンピュータは，校外に持ち出さない。やむを得ず，持ち出す場合は，別紙様式「情報機器持ち出し許可申請書」に記入し，移動時は常時携帯する。

③　情報を保存する媒体の持ち出しは十分に留意し，常に携帯する。

④　児童がコンピュータを利用する場合は，職員の監督下で行う。

⑤　職員が転任，退任する際には，本校の情報を持ち出したり，利用したりすることのないようにする。また校長は情報の持ち出しがないことを確認する。

(2) 物理的セキュリティ対策

①　「校内端末ＩＤ・パスワード」は，第三者に漏洩しないように留意する。

②　コンピュータは原則として施錠できる部屋に設置・保管する。

③　児童が使用するコンピュータには，漏洩しては困る情報資産を保存しない。

（3）技術的セキュリティ対策

① 職員用コンピュータでは，ログイン時に必ずパスワードを設定する。
② 個人情報等，重要度の高い情報資産は，電子メールでの送受信を行わない。
③ メールアドレスの入力に注意し。送信前はアドレスを再確認の上送信する。
④ 家庭で作成したファイルは，そのまま校用のコンピュータで読み込むとコンピュータウイルス感染の危険性があるので,**家庭用のコンピュータには必ずコンピュータウイルス対策ソフトウエアを常時稼働させておく。**
⑤ 受信した迷惑メールや不信なメールは開かないで削除する。
⑥ 職務に関係のないサイト，情報の発信源が不明なサイト，信頼できないサイトへのアクセスをしない。
⑦ 管理責任者の許可を得ずに，プログラムのダウンロードやインストールを行わない。新たにソフトウェアをインストールする場合は校務用パソコン install 報告書により申請をする。

（4）運用セキュリティ対策

情報システムの監視，情報セキュリティ対策の状況の確認等，運用面の対策をする。不測の事態が発生した時，千曲市教育委員会が定める情報セキュリティ管理責任者に速やかに報告し，適切な対策をする。

６　危機管理体制の整備

不測の事態に適切に対応するため，「情報の盗難，流出，漏洩事故への対応マニュアル」を作成する。

７　教職員の義務

教職員は，情報セキュリティポリシーを遵守する。

８　評価及び見直し

情報セキュリティの状況の変化に対応し，必要に応じて情報セキュリティポリシーの見直しを図る。

情報の盗難，流出，漏洩事故への対応マニュアル

- 学校から持ち出した情報が，自宅または通勤中に盗難にあった。
- 学校から持ち出した情報を紛失した。
- 学校のコンピュータがウイルスに感染し，情報が流出，漏洩した。

緊 急 対 応

- 直ちに事実を学校長に報告する。（いつ，どこで，何を，どれ位）
- 盗難，紛失の場合，警察に届ける。
- ウイルス感染の場合，ネットワークをとめる。

↓

関係機関への連絡

- 当該職員より事故情報を聴取する。
- 市教委，県教委，校長会に第一報を入れる。
- ネットワーク管理者（市教委）に連絡する。

↓

緊急対策会議

- 校長，教頭，教務主任，学年主任，情報教育担当職員で児童，保護者への対応を協議する。

↓

緊急職員会

- 事故の内容について，共通理解をする。また，協議した対策の役割分担をし，対応をする。
- ネットワーク管理者に対策を依頼する。

↓

緊急保護者会

- 事実を話し，謝罪とお詫びをし，対応をお話しする機会を持つ。

↓

事故報告書作成

- 保護者の意見，要望，課題も含めて，事故報告書を作成する。

↓

システム管理再点検

- ネットワークの復旧作業を行う。
- 情報セキュリティポリシーの見直しを行う。
- 秘密情報の分類，管理体制の見直しを行う。
- 児童，職員への再発防止の指導を行う。