

千曲市立屋代小学校 情報セキュリティポリシー

平成 21 年 10 月 13 日改定

(目的)

第 1 条 屋代小学校が保有する情報資産を様々な脅威から守るため、当校が行う情報セキュリティに関する対策の統一かつ基本的事項を定めることを目的とする。

情報資産：文書化されたものや電子的磁気的に記録された情報で教職員が校務遂行上利用しているもの

(対象範囲と対象情報資産)

第 2 条 この情報セキュリティポリシーの対象範囲は、教職員・児童（生徒）を含めた屋代小学校の情報資産の重要度（機密性）に即し、別に「情報資産リスト一覧表」を作成し、第 4 条（情報資産の取り扱い）及び第 5 条（出年始媒体による情報セキュリティ対策）に対応させるものとする。

(管理体制)

第 3 条 校長は情報セキュリティ対策の推進と情報セキュリティ管理体制の確立のために、情報セキュリティポリシーの策定、実施、監査および見直し等、継続的な運用及び改善に努めるものとする。

(情報資産の取扱)

第 4 条 情報資産の取扱にあたっては、以下の事項に留意する。

- (1) 情報資産は保存形態(紙・電子媒体)保存場所・閲覧(アクセス対象者)、保存期間重要度(保存区分等)による別紙屋代小学校情報資産リストを作成し、このリストに基づいて適正な管理を行うものとする。
- (2) 情報資産は、原則として複製及び校外へは持ち出しはしない。ただし、校務運営上やむを得ず持ち出す必要がある場合は、別に作成した『情報資産取り扱い要項』をもとに「情報持ち出し許可申請書」を提出して校長に申し出て許可を得ること。
- (3) 校外へ発信する情報については（文書化されたもの、電子媒体を問わず）、校長の許可を得ること。
- (4) 校務運営上、個人情報収集する場合は、目的・提供・管等を明らかにして、校長の許可を得ること。
- (5) 外部からの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こと。
- (6) 情報資産の保存について別に作成した「情報資産リスト一覧表」に基づき、保存期間や保存場所を明確にし、アクセス制限をハッキリさせたうえで、適正に保存すること。保存期間が終了したものは適正な方法で廃棄すること。

* 文書分類表に基づいて、職員室北側の棚に保存（分類表別紙 2）

(電子媒体等による情報セキュリティ対策)

第 5 条 情報資産を保護するために、次の情報セキュリティ対策を講じる。

(1) 人的セキュリティ対策

情報セキュリティに関する権限や責任及び遵守すべき事項を明確に定め、校長は職員研修を計画・実施し職員に対する周知及び徹底を図るとともに、十分な教育、啓発が行われるよ

うに必要な対策を講じる。

職員室・教室に配布された情報端末(以下校用コンピュータと言う)の利用に当たっては、不注意による破損・情報漏えい等がないように各校用コンピュータの管理責任者が責任持って管理する。

長時間の離席時には、コンピュータの電源を切るかログアウトする(短時間の離席時もスクリーンセーバーとスタンバイ時のパスワードをかけること)。

教室(特別教室も含む)において児童が情報端末を利用する場合は必ず担当職員の監督下で行うこと。

職員が転任、退任する場合は当校の情報を持ち出したり、情報資産を利用したりすることがないようにすること。また、校長は情報持ち出しのないことを確認すること。

校内ネットワークに関する各種サーバーについては、原則として複数の担当職員及び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が連携して管理すること。

(2) 物理的セキュリティ対策

情報機器を設置する施設への不正な立ち入り、情報資産への損傷、盗難等から保護するための物理的な対策を講ずる。

情報機器の盗難対策として、機器の固定や施錠できるラックでの保管等の対策をとること。

可搬型校用コンピュータは、管理責任者は退校時に鍵のかかるロッカーに保管(職員室北側ロッカー)し、盗難や情報漏えいのないような対策を行う。やむを得ず校外に持ち出すときは、別に定める規定により校長の許可を受ける。

校用コンピュータが設置してある職員室・コンピュータ室等は最終退校者が必ず施錠を行うことを原則とする。

災害への予防対策や不正侵入への予防対策をすること。

(3) 技術的セキュリティ対策

情報資産を不正アクセス等から保護するため、情報資産へのアクセス制御、ネットワーク管理等の対策を講ずる。

パスワード管理について

(a) 校用コンピュータの ID ならびにパスワードは第三者に漏洩しないように各自が管理すること。

(b) パスワードには、個人情報を使用せず、類推が困難なものを設定すること。また、他の者から見えるところに表示しないこと。定期的に変更すること。

電子メールの取扱について

(a) 個人情報等、重要度(機密性)の高い情報資産は電子メールでの送受信を行わないことを原則とする。

(b) 教職員へメールを送信するときは school office のメールアドレス宛に送信することを原則とする。

* 各小中学校の HP に記載されるメールアドレスは学校代表のアドレスとなっている。

(c) 添付ファイルの上限の容量は 8 MB 程度とする。また教育事務所等の県の機関では 1 MB が上限であるので、その範囲内で送信すること。

(d) 個人アドレスの使用は最小限に留め、所属アドレスを使用することにより情報を共有することに努めること。

(e) メールアドレスの入力には細心の注意を払い間違いのないようにすること。なお、「送信前確認」画面を表示し、再確認の上、送信することが望ましい。

(f) メールを複数の人に同時に送信する場合は、「宛先」「cc」は使用せず「bcc」を使用すること。

コンピュータウイルス対策について

校用コンピュータは、千曲市のサーバーにファイヤーウォールが設定されて、サーバー経由のファイルの送出入時にウイルスチェックや不適切なアクセス、侵入等に対応している。しかし、家庭で作成したファイルは、そのまま校用コンピュータに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、家庭の個人用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を常時稼働させておき、パターンファイルを最新の状況に保ちつこと。

インターネット利用について

(a) 職務に関係ないサイト、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や外部の情報システムへの不正アクセスを行わないこと。各自のインターネット利用状況についてはサーバーにlog(記録)が残ることを理解しておく。

(b) インターネットで情報発信する際には、他者の中傷・誹謗や公序良俗に反した発言はしないようにすること。

(c) 校用コンピュータはインターネットを利用したプログラムのダウンロードやソフトのインストールはできない仕組みになっているが必要な場合は校長を通して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相談すること。

(4) 運用セキュリティ対策

校長は自校の情報システムの監視、情報セキュリティの遵守状況の確認、セキュリティポリシーの運用面の対策を講じる。また情報システムに不測の事態が生じたときは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講じる。

(危機管理体制の整備)

第6条 校長は不測の事態に迅速かつ適正に対応するため、別に情報セキュリティ緊急対応マニュアルを策定するとともに、情報セキュリティ教育や定期的な訓練を行う。

(教職員の義務)

第7条 教職員は、情報セキュリティポリシーを遵守する義務を負う。

(監査)

第8条 情報セキュリティポリシーが遵守されていることを検証するため、適宜千曲市教育委員会は監査を実施する。

(評価及び見直し)

第9条 校長は情報セキュリティ監査の結果に基づき、セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、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。