千曲市立屋代小学校　情報セキュリティポリシー

1.　目的

本校が保有する情報資産を様々な脅威から守るとともに、情報セキュリティインシデントが発生したときに影響範囲を最小限にとどめ、正確かつ速やかに復旧するため、これらを利用する教職員等が遵守しなければならない事項を定めることを目的とする。

2.　組織体制

(1)　校長は本校の情報セキュリティ対策に関する権限及び責任を有する。

(2)　校長は、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、千曲市教育総務課長へ速やかに報告を行い、指示を仰がなければならない。

3.　資産の管理

(1)　情報資産の分類

情報資産は、次のとおり分類し、必要に応じて取扱制限を行うものとする。(該当する情報資産の詳細については、別表参照)

情報資産の分類

分類	分類基準	該当する情報資産のイメージ
重要性Ⅰ (機密性 3)	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。(秘密文書に相当する機密性を要する情報資産)	特定の教職員のみが知り得る状態を確保する必要のある情報で秘密文書に相当するもの 例)指導要録原本　職員人事関係書類 定期テスト　教育情報システム仕様書
重要性Ⅱ (機密性 2B)	セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす。(秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産)	教職員のみが知り得る状態を確保する必要がある情報資産 例)評定一覧表　定期テスト答案用紙 成績に関する個票 生徒指導・特別指導等記録簿 児童等の個人写真・集合写真
重要性Ⅲ (機密性 2A)	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす。(直ちに一般に公表することを前提としていないが、児童がアクセスすることを想定している情報資産)	教職員及び児童生徒同士のみが知り得る状態を確保する必要がある情報資産 例)出席簿　座席表　児童会名簿 地区別名簿　卒業アルバム 児童の学習記録 ロイロノート等の学習データ 学習活動の記録(動画・写真)
重要性Ⅳ (機密性 1)	影響をほとんど及ぼさない。	公表されている又は公表することを前提に作成された情報資産 例)学校・学年便り　年間行事計画 学校紹介パンフレット

(2) 管理責任

校長は、情報資産について管理責任を有する。

(3) 情報資産の分類の表示

教職員は、情報資産について、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

(4) 情報の作成

① 教職員等は、業務上必要のない情報を作成してはならない。
② 情報を作成する者は、情報の作成時に(1)の分類に基づき、当該情報の分類と取扱制限を定めなければならない。
③ 情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

(5) 情報資産の入手

① 学校内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。
② 学校外の者が作成した情報資産を入手した者は、(1)の分類に基づき、当該情報の分類と取扱制限を定めなければならない。
③ 情報資産を入手した者は、その情報資産の分類が不明な場合、校長に判断を仰がなければならない。

(6) 情報資産の利用

① 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。
② 情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。
③ 情報資産を利用する者は、電磁的記録媒体または保存されている領域(フォルダやサーバ)に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体または保存されている領域を取り扱わなければならない。

(7) 情報資産の保管

① 情報資産を保管する者は、情報資産の分類に従い、情報資産を適切に保管しなければならない。
② 情報資産を記録した USB 等の外部電磁的記録媒体を保管する場合は、外部電磁的記録媒体への書込禁止の措置を講じなければならない。
③ 重要性分類Ⅲ 以上の情報を記録した電磁的記録媒体を保管する場合、施錠可能な場所に保管しなければならない。

(8) 情報の送信

電子メール等により重要性分類Ⅲ以上の情報を組織外部(家庭や地域、事業者等)に送信する者は、限定されたアクセスの措置設定(アクセス制限や暗号化)を行わなければならない。

(9) 情報資産の運搬

重要性分類Ⅲ以上の情報資産を運搬する者は、校長に許可を得なければならない。また、運搬の際に不正利用を防止するための措置を講じなければならない。

(10) 情報資産の提供・公表

① 重要性分類Ⅲ以上の情報資産を外部に提供する者は、限定されたアクセスの措置設定を行わなければならない。

② 重要性分類Ⅲ以上の情報資産を外部に提供する者は、校長に許可を得なければならない。

③ 校長は、保護者等に公開する情報資産について、完全性を確保しなければならない。

(11) 情報資産の廃棄

① 情報を記録している USB メモリ等の電磁的記録媒体を廃棄する場合、電磁的記録媒体を初期化する等、情報を復元できないように処置をしなければならない。

② 情報資産の廃棄を行う者は、校長の許可を得なければならない。

4. 人的セキュリティ

(1) 教職員等の遵守事項

① 教育情報セキュリティポリシー等の遵守

教職員等は、千曲市教育情報セキュリティポリシー及び本校情報セキュリティポリシーを遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに校長に相談し、指示を仰がなければならない。

② 業務以外の目的での使用の禁止

教職員等は、業務以外の目的で情報資産の外部への持ち出し、教育情報システム(C4th、Home＆School、Google Classroom、ロイロノート等)へのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③ 情報の持ち出し

教職員等は、学校のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、別紙様式「情報資産持出許可申請書」に記入し、校長の許可を得なければならない。

④ 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

教職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、校長の許可を得て安全管理措置を遵守した上で利用することができる。(「支給以外のパソコン、モバイル端末及び電磁的記録媒体等の利用許可申請書」を提出して許可を得る。)

⑤ 机上の端末等の管理

教職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は校長の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

⑥ 退職時等の遵守事項

教職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

(2) 研修の実施

教職員等は、毎年度最低 1 回は情報セキュリティ研修を受講しなければならない。

(3) 情報セキュリティインシデントの報告

① 教職員等は、情報セキュリティインシデントを認知した場合、速やかに校長に報告しなければならない。

② 報告を受けた校長は、速やかに千曲市教育委員会に報告しなければならない。

(4) ID 及びパスワード等の管理

① 教職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

ア) 自己が利用している ID は、他人に利用させてはならない。

イ) 共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

② 教職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

ア) パスワードは、他者に知られないように管理しなければならない。

イ) パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

ウ) パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

エ) パスワードが流出したおそれがある場合には、校長に速やかに報告し、パスワードを速やかに変更しなければならない。

オ) 初期パスワードは、最初のログイン時点で変更しなければならない。

カ) 教職員等間でパスワードを共有してはならない。(ただし、共有 ID に対するパスワードは除く)

5. 技術的セキュリティ

(1) 電子メールの利用制限

① 教職員等は、業務上必要のない送信先に電子メールを送信してはならない。

② 教職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

③ 教職員等は、重要な電子メールを誤送信した場合、校長に報告しなければならない。

④ 教職員等は、指定されたシステム以外を用いて、業務における電子メールを送信してはならない。

(2) 暗号化

教職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性を確保することが必要な場合には、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

(3) 無許可ソフトウェアの導入等の禁止

① 教職員等は、業務上の必要がある場合は、千曲市教育委員会の許可を得てソフトウェアを導入することができる。なお、校長は、導入されたソフトウェアのライセンスを管理しなければならない。

② 教職員等は、不正にコピーしたソフトウェアを利用してはならない。

(4) 機器構成の変更の制限

① 教職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

② 教職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、千曲市教育委員会の許可を得なければならない。

(5) 業務以外の目的でのウェブ閲覧の禁止

教職員等は、業務以外の目的でウェブを閲覧してはならない。

(6) 不正プログラム対策

教職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

① パソコンやモバイル端末において、不正プログラム対策ソフトウェアの設定を変更してはならない。

② 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

③ コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、直ちに利用を中止しネットワークからの切り離しを即時に行わなければならない。

6. 運用

(1) 教職員等の報告義務

教職員等は、教育情報セキュリティポリシーに対する違反行為を発見した場合、直ちに校長に報告を行わなければならない。

(2) 法令等遵守

教職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令等を遵守し、これに従わなければならない。

① 地方公務員法(昭和 25 年 12 月 13 日法律第 261 号)

② 教育公務員特例法(昭和 24 年 1 月 12 日法律第 1 号)

③ 著作権法(昭和 45 年法律第 48 号)

④ 不正アクセス行為の禁止等に関する法律(平成 11 年法律第 128 号)

⑤ 個人情報の保護に関する法律(平成 15 年 5 月 30 日法律第 57 号)

⑥ 行政手続における特定の個人を識別するための番号の利用等に関する法律(平成 25 年法律第 27 号)

⑦ サイバーセキュリティ基本法(平成 26 年法律第 104 号)

⑧ 千曲市情報公開及び個人情報保護に関する条例(平成 15 年 9 月1日条例第 16 号)

7. 1 人 1 台端末におけるセキュリティ

千曲市教育委員会の策定するクロームブック利用ルールに基づき、学校内外での端末の運用ルールを制定しなければならない。

8. 監査

千曲市教育情報セキュリティポリシーおよび本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。

9. 評価及び見直し

校長は情報セキュリティ監査並びに情報セキュリティに関する状況の変化等をふまえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。