

情報管理について

1. 情報セキュリティポリシー基本方針

本校において取り扱う情報には、児童の個人情報のみならず、学校運営上の重要な情報が多数存在する。万が一、それらの紛失や漏洩等、事故が発生した場合には、極めて重大な結果を招くことになる。これらの情報及び情報を取り扱うシステムを様々な脅威から守ることは、学校運営上の重要な課題である。

したがって、児童の個人情報を保護し、情報に係る事故を未然に防止するために、本校としての情報セキュリティポリシーをもち、それに従って、実効性を伴った運用を図るものである。

全ての職員は、情報セキュリティの重要性に共通の認識をもつとともに校務の遂行に当たって情報セキュリティポリシーを遵守するものとする。

※ 情報セキュリティ・・・情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持すること。

※ 情報セキュリティポリシー・・・学校が掌握する情報資産に関する情報セキュリティ対策について、総合的・具体的にまとめたものであり、情報セキュリティ対策の根幹となるもの。

2. 組織

(1) 校内組織

- ① 情報統括責任者を校長とする。
- ② 情報セキュリティ管理者を教頭とする。
- ③ 情報システム管理者を情報教育主任とする。

(2) 役割

- ① 情報統括責任者は、学校におけるすべてのネットワーク、情報システム、情報資産及び情報セキュリティの統括的な権限及び責任を有する。
情報セキュリティポリシーの遵守状況の確認及び職員に対する指導を行う。
- ② 情報セキュリティ管理者は、情報統括責任者の指導のもと、情報統括責任者を補佐し、情報セキュリティポリシーの遵守状況に関する権限を有し、校内情報セキュリティの維持・管理を行う。
- ③ 情報システム管理者は、情報セキュリティ管理者の指導のもと、学校のネットワークや情報システム等の運用を司る。

3. 情報資産に係る遵守事項

※ 情報資産・・・情報システム及び記録データ。コンピュータから出力した紙媒体。
記録媒体（USBメモリ、ハードディスク、CD、DVD等）
諸表簿。成績物（通知表、テスト用紙、ノート、記録補助簿等）

- (1) 情報は校務目的の範囲内で利用すること。
- (2) 盗難や盗み見などによる情報漏洩を防ぐため、机上には情報資産を放置しないこと。
- (3) テストや成績物等を校内で扱う際にも、保管に留意すること。
- (4) 重要な情報資産を破棄する場合には、破棄するまで施錠管理された場所で保管し、溶解、裁断等で、情報が判読できないよう処理すること。

- (5) プリンタ、コピー、FAXから出力された文書は速やかに回収すること。
- (6) 重要な情報が記載されている用紙を、裏紙として再利用しないこと。
- (7) 職場では個人情報やID・パスワードなどの重要な情報資産に関する会話は、周囲に漏れることのないよう十分な配慮を行うこと。
- (8) 業務を遂行するため、やむを得ず外部に重要な情報資産を持ち出す場合は、必ず事前に校長の許可を得ること。また、外出時の行動については「4. 情報資産の持ち出しについて」に従って行動すること。

4. 情報資産の持ち出しに係る事項

- (1) 外部に重要な情報資産を持ち出すことは、原則禁止とする。
- (2) やむを得ず持ち出す必要がある場合は、別紙「個人情報の管理に関する分類について」に則り、以下(3)(4)を遵守すること。
- (3) 外部に重要な情報資産を持ち出す場合は、必ず事前に校長または教頭の許可を得て、「個人情報等資料使用記録簿」に記入すること。
- (4) 「使用期間」は原則1日とする。連続する2日以上持ち出す場合には、その都度1日ごとに許可を得ること。ただし、土日、祝日等、休日を挟む場合は、休日明けまで使用を認めるものとする。
- (5) 持ち出し時は、盗難・紛失等の情報漏洩リスクを常に意識し、手元から離さないように注意すること。
- (6) 記録媒体に格納されたデータについては、暗号化されたパスワードを設定するなど、セキュリティ対策を施すこと。また、学校外で利用するパソコンについてもセキュリティ対策を施すこと。学校外で利用するパソコンについてのセキュリティ対策については、「12. 学校外で利用するパソコンについてのセキュリティ対策」に従うこと。
- (7) 返却時は、「個人情報等資料使用記録簿」に記入し、持ち出した情報資産が全て揃っていることを確認し、不足があることが分かった場合は直に校長に報告すること。
- (8) 返却後、速やかに記録媒体のウイルススキャンを行うこと。

5. 離席時の対策

- (1) 机上にテスト類や成績物、名簿等紙ベースの資料を置いたままにしないこと。
- (2) 長時間離席する場合は、パソコンを正常に終了し、電源を必ず切ること。
- (3) パソコンを起動したまま、短時間離席する場合は、ハードロッキーを抜いたり、パスワード付きのスクリーンセーバー、又はパソコンのロックを設定したりするなど、他人に勝手に使用されないよう注意すること。
- (4) パソコンに重要なデータを表示している場合は、他人に盗み見されないよう周囲に配慮すること。

6. 情報システム機器利用時の遵守事項

- (1) 校務用コンピュータは、事務等の業務で使用するとし、割り当てられたコンピュータをその教職員だけが使用する。職員室の机上にワイヤーで固定し、鍵は情報セキュリティ管理者である教頭が管理する。
- (2) 教育用コンピュータは、児童生徒の学習のために活用する。教育用コンピュータを校務で使わないこと。
- (3) ハードウェアは、無断で改造したり、無断で他のネットワークに接続したりしないこと。
- (4) OSやソフトウェアにはセキュリティーホールという情報セキュリティ上の欠陥が発見されることがあるため、迅速に最新バージョンへの更新や修正プログラムを適用すること。
- (5) 学校内で利用できるパソコンは、校務用コンピュータ及び教育用コンピュータのみ使用可能とし、個人所有のコンピュータ（タブレット等を含む）を無断で持ち込まないこと。持ち込む場合には、「個人端末持込み許可願」を校長に提出し、許可を得ること。

7. ソフトウェアの取扱い

- (1) ソフトウェア等を教育委員会の許可なしにパソコンにインストールしないこと。
- (2) ソフトウェアの違法コピーを行わないこと。
- (3) 学校がライセンス所有するソフトウェアを個人所有のパソコンにインストールしないこと。

8. インターネット利用における遵守事項

- (1) 職務に関係のないホームページの閲覧を行わないこと。
- (2) アクセスしたホームページが有料か無料かの確認を行うこと。
- (3) インターネットからむやみにファイルのダウンロードを行わないこと。
- (4) インターネットの掲示板に書き込みを行わないこと。

9. 電子メール利用時における遵守事項

- (1) 職務以外の目的で電子メールを使用しないこと。
- (2) 付与されているメールアドレス以外を使用しないこと。
- (3) メールを送信するときは「内容」と「宛先」の確認を必ず行うこと。
- (4) 個人加入のメールアドレスへむやみに転送しないこと。
- (5) データ量が大きいサイズのメールは送信しないこと。
- (6) 不審なメールを開封したり、添付ファイルを実行したりしないこと。
- (7) 原則として重要な情報はメールで送信しないこと。業務を遂行するため、やむを得ず送信する場合は、必ず事前に校長の許可を得ること。

10. コンピュータウイルスに対する遵守事項

- (1) コンピュータウイルス対策ソフトの定義ファイルは常に最新の状態を保つこと。
- (2) 無関係の人から送信された電子メールや添付ファイル、ダウンロードや外部から持ち込まれたプログラムなどを開く場合は開く前にウイルス検査を行うこと。
- (3) ウイルス感染被害に備え、必要に応じて日頃からデータのバックアップを行っておくこと。
- (4) コンピュータウイルスの感染を発見した場合は、校長に直ちに伝え、校長は学校教育課長あて連絡すること。

11. フィルタリング解除

- (1) インターネットサイトのフィルタリング解除は原則として禁止とする。校務上、事情がある場合には、校長を通して、学校教育課と相談し、許可を得た後、指示された手順で解除を行うこと。また、校務終了後、フィルタリングをかけること。

12. 学校外で利用するパソコンについてのセキュリティ対策

- (1) 自宅で使用する個人のパソコンにも必ずセキュリティ対策ソフトをインストールし、常に最新パターンファイルに更新したり、修正プログラムの適用をしたりしながら、セキュリティ対策を怠らないこと。
- (2) 自宅で使用する個人のパソコンのハードディスクには、重要情報の保存を決して行わないこと。
- (3) ファイル交換ソフト(Winny 等)がインストールされている自宅で使用する個人のパソコンでは、個人情報や職務上重要な情報を扱わないこと。

13. 情報セキュリティ事故発生時の実施手順

- (1) 職員は、情報漏洩、紛失、盗難、ウイルス感染等の情報セキュリティ事故が発生した場合は、速やかに校長に報告すること。
- (2) 校長は、「事故報告書」により、教育長あてに報告すること。

学校から児童の個人情報が増失、流出、漏洩した場合、学校への信用を失墜させ、場合によっては損害賠償を請求される可能性もあります。

教職員には、条例による罰則や、地方公務員法に基づく懲戒処分が課せられることもあります。

教職員は、「ふじみ野市民の大切な情報を扱っている」という意識をもち、情報セキュリティポリシーを遵守しましょう。

別紙

個人情報の管理に関する分類について

分類	管理方法	個人情報の具体内容（すべての記録方法を対象とする）
I	持ち出し禁止	【学籍関係】 ○指導要録（学籍に関する記録） ○出席簿 ○卒業証書授与台帳 ○除籍簿 ○転退学簿 ○転入学簿 ○就学児童異動報告書 ○教科用図書給付児童名簿 ○要・準要保護児童認定台帳 ○就学援助関係書類 【成績関係】 ○指導要録（指導に関する記録） ○評定一覧表 ○成績に関する個票等 【指導関係】 ○事故報告書及び記録簿 ○特別支援教育関係の一覧表及び個票、記録簿等 ○指導上の配慮を要する児童の一覧表及び個票、記録簿等 ○児童生徒の写真 【進路関係】 ○卒業生進路先一覧等 ○中学校入学者選抜に関する表簿（願書等） 【保健関係】 ○健康診断に関する表簿（健康の記録）及び歯の検査表 【その他】 ○学校の児童住所録・緊急連絡網 ○放課後子ども教室関係の住所録 ○学校行事等の招待者住所録 ○健康保険証等の写し（移動教室時の持出は可） ○区域外就学願及び住民票 ○学校沿革誌 ○旧職員住所録
II	持ち出す都度 校長または教頭の承認を得る （個人情報等資料使用簿）	【成績関係】 ○通知表 ○答案用紙、作品等（作文やレポート等）、成績処理に必要なデータ 【指導関係】 ○児童指導の記録等（分類 I を除く） ○週ごとの指導計画（週案）・個人情報の記載がある場合 ○緊急連絡網 【進路関係】 ○調査票及び推薦書 【その他】 ○担当学級の児童生徒住所録 ○担当学級指導の緊急連絡網 ○職員の住所録・緊急連絡網 ○各種名簿

※この分類表にない児童の個人情報の扱いについては、校長または教頭に確認すること