

椎葉村立不土野小学校 情報セキュリティポリシー

情報セキュリティポリシーは、本校で保有する情報資産（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用いるもの）を様々な脅威から守るため、その基本的な考え方や運用体制、具体的な対策等を定めたものである。

【1】適用範囲

情報セキュリティポリシーの適用者は、教職員・児童を含めた本校の情報資産を利用するすべての者を対象とする。

【2】情報資源の統括

校長は、校内・校外を問わず情報資源の保管・保存にあたり、棄損・滅失・改ざん・漏えい等が生じないよう注意し、校内・校外を問わず情報資産の管理を統括し、適正かつ円滑な運営を図らなければならない。

【3】情報資産の取り扱いについて

- (1) 情報は原則として、校長の承認を得ないで複製および、校外持ち出しをしてはならない。
- (2) 校外へ発信する情報については、校長の許可を得た上で行う。
- (3) 校務運営上、個人情報を収集する場合は、目的・提供・管理について校長の承認を得る。
- (4) 外部から電話等での問い合わせがあった場合、原則として個人情報の提供はしない。
※ 特に電話番号等については相手の電話番号を確認し、こちらから連絡し直すようにする。
- (5) 外部からの情報開示請求については、椎葉村の個人情報保護条例により対応すること。
※ 椎葉村教育委員会の指示による。
- (6) 情報資産の処理を端末で行う場合は、校内LANに接続されたコンピュータで行い、校内サーバーの指定されたフォルダに保存する。
- (7) 情報資産の保存については「文書分類表」に基づき適正に保存し、保存期限を明確にした上で保存する。保存期間が終了したものは校長に決裁を受けた上で、情報区分により適正な方法で廃棄する。 本校秘密情報の取り扱いについて
- (8) 機密情報については「のとおり取り扱う。

【4】情報端末の取り扱いについて

- (1) 職員用情報端末の利用にあたっては、破損等がないように各自が責任をもって管理する。
※ 不注意による破損等が生じた場合は、速やかに校長に連絡するとともに、自己責任で正常な状態に回復させること。
- (2) 職員用情報端末は、原則として校外に持ち出さないこと。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、別紙様式「不土野小学校秘密情報持ち出し許可申請書」に記入し、校長の承認を得た上、必要最低限の情報が保存された端末（情報にはパスワードをかけ、暗号化する）を持ち出すことができる。
- (3) 長時間の離席時には、パソコンの電源を切るかログアウトし、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。
- (4) 児童が教室（特別教室含む）において情報端末を利用する際は、管理者権限での使用を禁止し、原則として担当職員の監督の下で行う。
- (5) 職員が転任、退任する際には、情報を全て消去し、転任後は本校の情報資源を利用することがないようにする。
- (6) 校内ネットワークに関わる各種サーバーについては、情報管理・情報教育担当職員（複数名）が連携して管理する。

【5】パスワード管理について

- (1) 職員用端末のパスワードは、【起動時のパスワード】と【ログイン時のパスワード】を別々に設定する。
パスワードは、記憶しておくことが基本であるが、忘れないよう記録する場合は他人に見られない場所に厳重に保管する。 なお、情報管理係は最新の【校内端末ID・パスワード一覧表】を作成し厳重に管理する。
- (2) 【校内端末ID・パスワード一覧表】は、校長・教頭・情報管理・情報教育係以外の第三者に漏洩しないよう鍵のかかる金庫に保管する。

[6] メールの利用について

- (1) メールの利用については、教育活動に限定し、私的メールは行わない。
- (2) 学校代表のメールアドレスは、文書係で受信し必要により印刷回覧または転送する。
- (3) メールは送信後の取り消しができない。メールアドレスの入力には細心の注意を払い間違いないようにする。
- (4) メールを複数の人に同時に送信する場合は、「宛先」「CC」は使用せずに「BCC」を使用する。
※ 「BCC」では他の人のメールアドレスが送信されることはない。

[7] コンピュータウイルス対策について

- (1) ウイルス対策ソフトは、常駐設定し、パターンファイルを常に最新に保つこと。
- (2) メールに添付されてきたファイルは、安全性が確認できないものは開かないこと。
- (3) 個人用端末や個人用電子記録媒体によるウイルスの持込をしないよう注意すること。
- (4) 自宅PCから学校のPCへのメール送信は、ウイルスの持込の可能性があるため、行わないこと。
- (5) OS (Windows) には、最新のセキュリティパッチを当てること。
- (6) 情報管理係は毎朝、定期的にサーバーのウイルスソフトでクライアントの状況を確認すること。
※ 情報の漏れる最大の原因は「公私混同」
 - ◎ 情報の漏れる原因
 - ① 一人の判断でソフトをインストールしない。
 - ② 信用できないサイトから感染を防止する。
 - ③ ファイル交換ソフト等は使用しない。

Winny、Keylo99er、spyware、SPAM、Bot、Phishing etc.

[8] 秘密情報以外の教育情報の取扱い

- (1) 原則として、指定されたフォルダにのみ保存する。特に公開されていない情報については、取扱いに十分注意する。
- (2) 個人機器に校務のデータを保存したままにせず、校内サーバーに保存して情報資産として共有する。
- (3) データの作成にあたっては、学校の情報資産として共有して複数年にわたり活用することを前提に、校内LANに導入されたソフトウェアで作成し保存する。

[9] WebSite(ウェブサイト)公開に関するガイドラインについては別に定める。

[10] 著作権の保護について

- (1) 校内LANに接続しているパソコンにインストールするソフトウェアは、正規のライセンスを有すること。
- (2) 校内LANに接続しているパソコンにソフトウェアをインストールする際は、事前に情報管理係に申し出て許可を得る。借用、サンプル、フリーソフトも同様とする。
- (3) 教育活動と著作権については著作権侵害とならないようする。

[11] 情報機器トラブル時の対応例

- (1) 機器トラブル、ネットワークトラブル、ウイルス感染等トラブルが生じた場合は、速やかにLANケーブルを抜いた上で、情報教育係に連絡する。
- (2) 情報教育係は、校長に報告し、指示を得て村教育委員会連絡する。
- (3) 個人情報漏洩等の被害が予想される場合には、校長は速やかに村教育委員会に連絡する。
- (4) 校長は保守業者（村教育委員会）の指示に従い、ネットワークを切り離す等の初期の対応を行う。
- (5) 保守業者が来校し対応を行う。

[12] 校内サーバーの取り扱い

- (1) サーバー管理者は、責任をもってウイルスを駆除する。

椎葉村立不土野小学校機密文書・データ持ち出し許可申請書

＜注意事項＞

- 1 この申請書は本人が直接持参し、必ず校長の承認を得る。
- 2 機密情報漏洩をさせないよう細部に注意を払う。
- 3 移動時は常時携帯する等、車内や人目に付く所への放置はしない。
- 4 学校のPCは原則として持ち出し厳禁である。
- 5 持ち出しの目的完了後、速やかに所定の場所に戻し、目的外使用はしない。
原則として申請日の次の日には返去する。
- 6 個人持ちのPC、FD、CD-R(RW)、DVD、USBメモリ等の端末(記憶メディア)で機密情報を持ち出した場合は印刷の後、確実に内容を消去し、情報管理係に確認をしてもらう。尚、個人持ちの記憶メディアには暗号化及びパスワード等のセキュリティロックをかける、暗号化するなどの対策を確実に施す。
- 7 機密情報ファイルはいかなる場合であってもメール添付及び送受信しない。
- 8 情報の移動中に事故があった場合は、速やかに校長に報告する。

＜記入例＞

椎葉村立不土野小学校機密文書・データ持ち出し許可申請書

椎葉村立不土野小学校 ホームページ運用に関するガイドライン

1 ホームページ公開の目的

- (1) 不土野小学校における教育活動を広く紹介し本校及び本校の教育について理解・協力を得る。
ex. 学校、行事、児童の活動等の紹介、PTA活動の紹介等。
- (2) 情報発信により、地域に開かれた学校の一端を担う。
- (3) インターネット上での交流の窓口とし、他校との共同学習の場を作る。
- (4) 児童自らが学習の成果を発信する場とし、自己表現力、情報発信能力の育成を図る。

2 ホームページ運用校内組織

(1) 公開情報

- ・ 公開情報は、公開前にデジタル情報管理係及び校長が確認する。
- ・ 校長の許可のもと、各分担、分掌の責任の範囲において運用を認める。その運用は、職員全体で確認する。
- ・ 「インターネット利用のガイドライン」を遵守しており、各分担、分掌の範囲で公開が許されると校長が判断する内容であるもの。
- ・ 公開の目的が教育活動の一環であることを校長が認め、運用する。

(2) 公開の手順

- ・ 公開希望者は、公開予定ページを用紙に印刷するか、または、校内のコンピュータで閲覧できる状態にして校長及びデジタル情報管理係に提示する。
- ・ 校長及びデジタル情報管理係は、公開にふさわしい内容、条件を備えているか吟味し、判定する。
- ・ 校長及びデジタル情報管理係は、判定結果とその理由を速やかに申請者に連絡する。
- ・ 公開の承認を得た場合、申請者・デジタル情報管理係は、速やかに公開作業を行う。

(3) ホームページのアップロードや更新に使用するコンピュータは、職員室の共用のコンピュータ及び学校に配備されているコンピュータとする。

3 本校児童の個人情報保護に関する事項

(1) 発信する個人情報の扱い

- ・ 本校作成の「インターネット利用に関する規定」による。

(2) 受信した個人情報の扱い

- ・ 情報通信ネットワークを利用して入手した個人情報については、適正な利用に努めると共に教育以外の目的での利用、提供及び複製は行ってはならない。

(3) 不要となった個人情報の廃棄

- ・ 情報通信ネットワークの教育活用の目的を達成するために使用された個人情報は、その目的が達成された時点で確実に破棄する。

(4) その他

- ① 校長は、校内の全教職員に対し、次の内容についての研修を積極的に実施し、情報通信ネットワークの適切な利用に努める。
 - ・ 情報通信ネットワークの利用における個人情報、著作権保護等に関すること。
 - ・ 情報通信ネットワークの特性を考慮した有害情報の取り扱い等倫理に関すること。
 - ・ その他利用に当たっての管理及びセキュリティーに関すること。
- ② 児童が情報通信ネットワークを利用する場合には、教職員は、児童に対して次の内容について指導する。
 - ・ 情報通信ネットワークの利用における個人情報、著作権保護等に関すること。
 - ・ 情報通信ネットワークの特性を考慮した有害情報の取り扱い等倫理に関すること。
 - ・ その他利用に当たっての管理及びセキュリティーに関すること。

4 著作権に関する事項

- (1) 児童の作品は、教育活動の情報提供に有効であり、かつ校長が発信してもよいと判断した場合、本人の許可を得てこれを公開することができる。第三者の転用は認めない。
- (2) 著作権フリーのデータやソフトであっても、勝手に内容の改変、作者名の改変等をしてはならない。
- (3) 授業等に活用する場合は、提供条件を確認し、作者の権利を不当に侵害しないように留意する。

機密情報漏洩時の対応

- 1 機密情報の紛失・盗難・漏洩及びその可能性がある場合は、速やかに校長に報告する。
- 2 校長は、直ちに村教育委員会、関係機関に報告し対処する。また、その原因を究明と事後の対策を検討する。
- 3 校長は村教育委員会と連携し、保護者等に速やかに事実の報告と謝罪を行う。

＜機密情報具体的運用事項＞取り扱い方法

取り扱い方法	データ	書類	端末	注意事項
校外へのメール	禁止			誤送信による情報漏洩を防ぐ。ただし、指定された場合は、校長の許可を受けた上で相手方に電話連絡をした直後に送信する。
校内へのメール	禁止			誤送信による情報漏洩やデータの分散を防ぐ。
FAX送信		禁止		誤送信による情報漏洩を防ぐ。ただし、指定された場合は、校長の許可を受けた上で相手方に電話連絡をした直後に送信する。
送付 (郵便・宅配)	破損しないよう 包装した上で送 付する。	厳重に封をし、発 送記録をつける。	禁止	親展印を押印の上、発送し たことを記録する。
保管	校内サーバーに 保管すること。	鍵付きの書庫・金 庫に保管する。	鍵付きの机に保 管する。	データを保存する場合はパ スワードと責任者の設定を する。
持ち出し(校外)	校長の許可を得 た上、必要最低 限の情報だけを 帶出できる。	校長の許可を得 た上、必要最低限 の情報だけを帶 出できる。	校長の許可を得 た上、必要最低限 の情報だけを帶 出できる。	機密情報を持ち出す場合 は、「不土野小学校機密情 報持ち出し許可申請書」で 事前に校長の許可を得る。
コピー	バックアップコ ピーを除き禁止	保存用を除き原 則禁止		
廃棄処分	物理的に破壊	シュレッダー処 分		機密文書については、村教 育委員会の指示により実施 する。