大府市立共長小学校情報セキュリティポリシー

２０２０年４月１日

前　　文

学校ではさまざまな個人情報や教育情報を扱っている。近年デジタル化した情報も多くなっている。しかし、デジタル化された情報はネットワークの外部からの不正アクセスや教職員の過失等により、常に漏えいの危険と背中合わせの状態にある。そのため、学校の情報を保護し適切に管理・運営することが重要になっている。

そこで本校では「大府市小中学校における情報セキュリティポリシー（基本方針）」を基本に別途「大府市立共長小学校セキュリティポリシー」を定め、情報の保護・管理・運営を適切に行うものとする。

このセキュリティポリシーを守るべき対象者は、本校の教職員・臨時職員・講師・事務職員とする。

Ⅰ　情報セキュリティ確保のための体制の確立

情報統括責任者（校長）を委員長とする情報セキュリティ委員会を組織し、全校レベルで情報管理に関する積極的な活動を行う。

１　組織の構成

情報統括責任者（校長）、情報セキュリティ管理者（教頭）、個人情報保護事務取扱者（教務・校務）　学年情報セキュリティ管理者（学年主任）、ネットワーク管理者（情報主任）で構成する。

２　組織の役割

①　セキュリティポリシーの策定
②　導入・運用
③　評価・見直し
④　セキュリテイポリシーの改訂・発展

Ⅱ　情報セキュリティ確保に必要な対策の実施

１　物理的セキュリティ

①　サーバーは常に施錠し、不正な立ち入り及び損傷等から保護する。
②　貸与されたパソコン及び記録媒体については適切に管理し、退校時には外部から目の届かない所に適切に保管する。

２　人的セキュリティ

①　職員は、情報セキュリティポリシーの内容を遵守しなければならない。特に遵守が必要な事項についてはセキュリティポリシーの誓約書をセキュリティ管理者（教頭）に提出しなければならない
②　個人情報を扱う場合、不必要な閲覧又は第三者への不当な開示及び漏洩をしてはならない。（情報統括責任者の許可）を得る。
③　個人情報を電子メール等により外部に提供してはならない。
④　個人情報（大府市個人情報分類１・２）の入った記録媒体の持ち出しはできない。個人情報を含まないデータ（大府市個人情報分類３）の持ち出しについては、セキュリティ管理者（教頭）の許可を得て、専用ＵＳＢを使用する。
⑤　職員が異動・退職等により業務を離れる場合には、知り得た情報を外部に漏らしてはならない。

⑥　転入および新規採用職員は情報セキュリティ管理者（教頭）が行う情報セキュリティ研修会に参加しなければならない。
⑦　職員はセキュリティポリシーに関する問題が発生した場合は速やかに情報セキュリティ管理者（教頭）に報告し、助言または指示を仰ぐ。

【参考：大府市における個人情報重要性分類】

	重要性分類	備　考	例
1	個人情報並びに業務上必要とする最小限のもののみが扱う情報（極秘の情報を含む）	機微情報	疾病履歴、補導歴、家庭環境、指導要録など
2	公開することを予定していない情報（秘の情報を含む）	いわゆる個人情報	児童・生徒氏名、保護者氏名、住所、連絡先が一覧になったもの 児童・生徒の個別の評価項目における結果、所見など
3	上記以外の情報	個人情報を含まないと解される情報	※個人情報を明らかに含まないデータに加えて、次のような例も３に分類します。 児童・生徒名のみを含むファイル、肖像を含む写真データ、職員・児童・生徒のデジタル作品（著作物であり個人情報の混入確認が困難）

３　技術的セキュリティ

①　ネットワーク管理者はネットワークが停止しないように常に監視と管理を行う。
②　職員は校務目的以外に情報機器及びネットワークを使用してはならない。
③　職員は、私的パソコンをネットワークに接続してはならない。
④　職員は、使用するパソコンに許可なくソフトウエアーをインストールしてはならない。
⑤　職員は、使用するパソコンや情報システムに改造等を行ってはならない。
⑥　職員は、ウイルスチェックを実施していない外部メモリー等を使用するパソコンに接続してはならない。
⑦　不正アクセスを防止するため、本校の情報を使用するすべての者は、適切なパスワードの管理を行わなくてはならない。
⑧　**自宅で使用するパソコンについてもウイルス対策用ソフトを導入する。また、常に最新のものに更新する。**

４　紙媒体における個人情報の管理

①　外部から来る人（ＰＴＡ、ボランティア、業者）及び児童などの目が届くところ**（机上等）には個人情報を含む書類は置かない**。
②　厳重に保護すべき**個人情報関係書類は、㊙の印**を押す。
③　パソコンを**保管する際には、引出しに入れる、覆いをかける**などして、外部の目に触れないようにする。

●職員室内書庫の施錠できるロッカーに保管するもの

指導要録、通知表、卒業台帳・修業台帳、成績一覧表、家庭環境調査票、児童引き渡し調査票、すくすく個票、顔写真

＊その他生徒指導関係の書類、特別支援関係の書類等個人情報を含む書類については書庫内のスチールロッカーに保管する。

●保健室で施錠をして保管

健康管理・指導カード

●校長室内にある施錠できるロッカーに施錠して保管

卒業アルバム、文集、氏名が記載された意見集等

●施錠できる職員の引き出し

児童関係書類（成績資料を含む）、学級経営案等個人情報を含む書類

5　コンピュータ・ネットワークの利用

① スクリーンセーバーからの復帰時にはパスワードの入力を必要とするように設定する。
② 個人情報を電子メール等により外部に提供することはしない。
③ インターネットメールの私的利用は禁止する。
④ 情報を用紙として、プリンタ・コピー等で出力した場合は放置せず，直ちに取りに行く。
⑤ パソコン内にはデータを保存しない。必ず，サーバーに入れて保存する。
⑥ 作業を終えるときには施錠のできる引き出し等に保管する。

6　個人情報の持ち出しについて

① 学校から持ち出し禁止のもの（学校で作業するもの）
指導要録，ユーザーＩＤ・電子メールアドレス等，その他情報セキュリティ委員会で定めたもの
② 「個人情報持ち出し管理簿」に記入して持ち出し可能なもの
各種名簿，答案用紙，通知表等，成績に関する書類，学年・学級経営等の書類
③ 保存・公開について細心の注意を払うもの
卒業アルバム，文集・氏名が記入された意見集，ビデオテープ，写真等

＊持ち出しは紙媒体・専用ＵＳＢに限る。
＊個人情報を持ち出す際には，寄り道をしない。

7　個人情報を持ち出すときの手順

【持ち出すとき】

① 「個人情報持ち出し管理簿」（教頭保管）に必要事項を記入する。

② 「個人情報持ち出し管理簿」を情報セキュリティ管理者（教頭）に渡し，持ち出す物の確認を受ける。

③ 情報セキュリティ管理者（教頭）は、情報統括責任者（校長）の許可を得る。

【返却するとき】

① 「個人情報持ち出し管理簿」に必要事項を記入する。

② 「個人情報持ち出し管理簿」を情報セキュリティ管理者に渡し、持ち出した物の確認を受ける。

8　自宅のコンピュータについて

① 学校から持ち出したデータについては、専用ＵＳＢ内で作業し、自宅のコンピュータにはデータを保存しない。

② 作業をするときは，コンピュータはネット環境から切り離す。

9　保有個人情報の廃棄について

① 紙資料は，シュレッダー処理をする。古紙として利用しない。

② デジタル記録媒体の個人情報は保存期間終了後に全て廃棄する。

＊個人情報廃棄の際は，直接本人が行う。

10　その他ICT機器について

○　個人情報が含まれる備品については施錠のできる場所に保管する。

附　　則

この情報セキュリティポリシーは２０２０年４月１日から施行する。