

沖縄県立那覇みらい支援学校 【個人情報保護方針】

本校では、個人情報の重要性を認識し、沖縄県個人情報保護条例並びにその他関係法令等を遵守し、以下の方針に基づき個人情報の保護に努めます。

ここでいう個人情報の例

※教育委員会「学校における個人情報の保護方針及び危機管理の策定について」参照

○基本的事項：氏名、性別、生年月日、年齢、続柄、住所、電話番号、本籍

○心身の状況：健康状態、病歴、心身的特性・能力

○家庭生活：家庭状況、婚姻歴、親族関係

○社会経済活動：職業・職歴、学歴、資格・賞罰、財産、所得、金融取引関係

○内心の状況：思想、信教、信条、趣味・嗜好

うち、病歴、思想、信条は機微情報であり、特に取り扱いに注意が必要。

1 個人情報の取得について

本校は、個人情報を取得する際には利用目的を明確にし、その上で適法かつ公正な手段によって個人情報を取得します。

2 個人情報の利用について

本校は、取得した個人情報を、取得する際に明示した利用目的の範囲内で利用します。

3 個人情報の第三者への提供について

本校は、本校規約や法令等に定める場合を除き、取得した個人情報を事前に本人に同意を得ることなく第三者に提供しません。

4 個人情報の安全管理について

本校は、個人情報の紛失、破壊、改ざん・漏えい等を防止するため、必要かつ適正な安全管理措置を講じます。

5 個人情報の第三者への委託について

本校は、個人情報取扱事務を外部に委託する場合は、当情報が安全に管理されるよう必要な措置を講じます。

6 個人情報の開示・訂正・利用停止について

本校が保有する個人情報について、その本人からご自身に関する個人情報の開示・訂正・利用停止の依頼があった場合は、法令等に基づき適正に対応します

はじめに

過去に、PC(iPadも含)の盗難、コンピュータウィルスの感染、USBの紛失による個人情報の漏洩が発生しており、大きな社会問題になっています。特に学校においては、教育目標を達成のため、児童生徒の氏名、住所、電話番号、成績及び健康状態など非常に多くの個人情報を扱っています。教職員一人一人が、個人情報の所得・利用や保管方法など、個人情報の扱い方について正しい知識を身につけ、個人の権利利益の保護に努めなければなりません。

1 学校における個人情報

- (1) 学籍関連 ①生徒名簿 ②出席簿 ③指導要録 ④同窓会名簿
- (2) 生徒指導関連 ①在校生顔写真 ②生徒住所録 ③生徒緊急連絡網
- (3) 成績関連 ①通知票 ②通知票伝票
- (4) 進路関係 ①進路結果 ②調査書
- (5) 保健関連 ①健康診断書 ②保健調査書 ③学校生活管理指導表
- (6) 事務関連 ①教職員履歴カード ②給与等支給明細書 等々

2 卒業生の個人情報の取り扱いについて (R4年度確認事項)

- (1) 小・中学部は紙媒体・SVデータ共にそれぞれの学部引き継ぐ。
- (2) 高等部卒業生の個人情報の取り扱いについて
 - ① 教育課程係が個人情報を一括してCD-Rに保存し、SVからは完全に抜き取る。
 - ② CD-Rは校長室金庫保管とし、進路指導部主任が5年間管理する。
 - ③ 5年経過後は情報漏洩が起これないようにCD-R自体を破碎して破棄する。

3 一般的な個人情報漏洩につながる脅威例および、大切な個人情報を守るためには

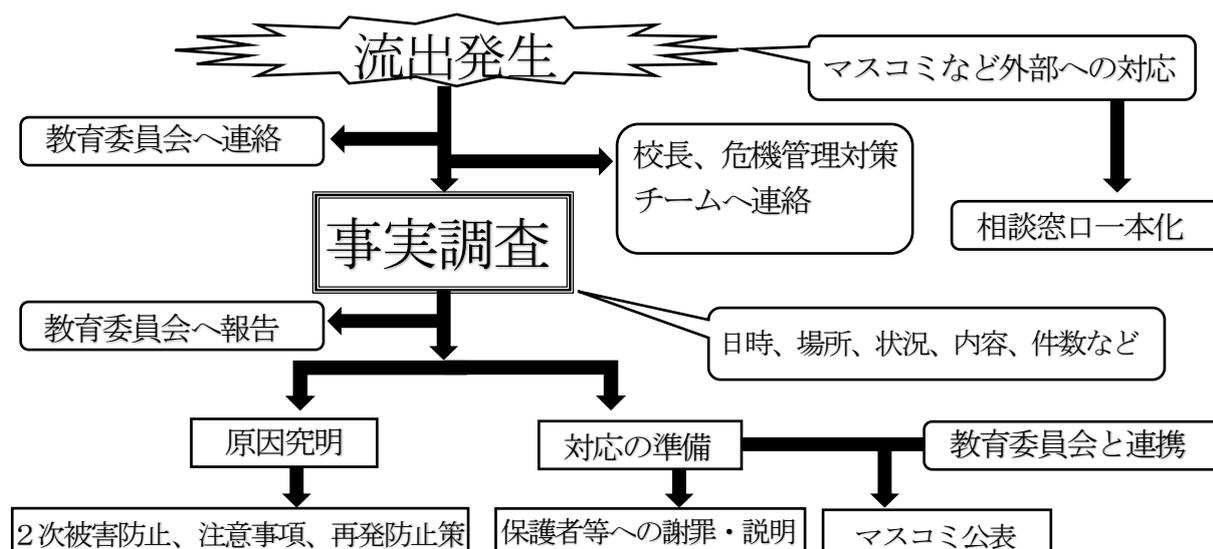
- (1) 校務用パソコンの盗難、紛失による漏洩、またUSBメモリなどのメディアの盗難、紛失による個人情報漏洩→ **個人情報の持ち出し許可申請 (別紙1号)**
- (2) 学校ホームページへの個人情報掲載による漏洩
→ **学校における個人情報公開に関する許諾書 (別紙2号)**
 - ① 許諾書を書いてもらい、家庭訪問や個人面談時に必要事項(学校・学年だより、情報メディア、作品展示会・各種コンクール等)の確認を行い、コピーは個人ファイルに綴り、原本は各学部の情報係に提出。情報係は、取りまとめて教頭(情報関連担当)に提出。原本は、教頭保管とする。
 - ② 児童生徒の作品展示会や各種コンクールの場合、学校名、学部名、氏名の個人情報が掲載されることがあるため、各教科や出展等の担当の係で再度確認後、出品を行う。
- (3) メールやチャットの誤送信による漏洩
→ メールやチャットで送信する際は、相手先のメールアドレスをしっかりと確認。

- (4) 学校内パソコンのウィルスやスパイウェア感染による漏洩
→ Windows 更新プログラムのインストールや定期的にあるアップデートの習慣化。
- (5) 情報機器処分時のデータ消し忘れによる漏洩
→ 情報機器処分の際は、データ消去を確認。
- (6) 個人情報が入ったUSBなどの利用
→ 原則、USBは学部で1つ割り当てられていますので、それを使用します。

4 個人情報流出時の危機管理マニュアル

- (1) 危機管理対策チームメンバーの選定 個人情報流出に関する事実調査、原因究明、対応の準備などを行う。教頭、事務長、各主任、情報担当者などで構成する危機管理対策チームのメンバーの選定をする。
- (2) 事故発生時の報告・連絡の手順
事故発生→教頭→校長→危機管理対策チームなど、報告・連絡の手順を定める。また、随時教育委員会への連絡・報告を行い密に連携を取る。
- (3) 対応窓口の一本化
- (4) 事実調査
- (5) 原因究明
 - ① 二次被害の防止、将来の発生可能性について
 - ② 再発防止策（安全管理策など）
- (6) 事後の対応
 - ① 今後の方針（対策の方針など）
 - ② 児童生徒・保護者への謝罪・説明
 - ③ 公表

○緊急対策の流れ図



5 今すぐ出来る情報セキュリティー向上対策

- (1) フォルダーにパスワードをかけるソフト「ED」（フリーソフト）
<http://www.vector.co.jp/soft/win95/util/se119287.html>

(2) リース返却、売却または処分時には、データの完全消去をする為のソフト（フリーソフト）
Eraser（英語版）・・・<http://www.tolvanen.com/erase>