個人情報の紛失防止について

・　個人情報の複製や学校外への持ち出しは原則禁止されています（各市町村立学校については、それぞれの市町村の規定による）。
・　個人情報の紛失は、児童生徒・保護者のプライバシーの侵害であり、情報の漏洩により、詐欺などの二次的な被害をもたらす恐れがあることなどから、特に慎重な取扱いが求められます。

○　次の事例は、ある小学校に勤務する女性教諭の典型的な個人情報紛失事故の例です。

教諭Ａは、担任児童の試験結果の集計を自宅で行うため、校長の許可を得ずに、個人情報が記録されたＵＳＢメモリを鞄に入れ退勤した。
帰宅途中、買い物のためショッピングセンターに立ち寄り、鞄を車内に置いたまま自家用車を駐車場に止め、１０分後、自家用車に戻ったところ、助手席の窓が割られ、車内に置いてあった鞄が盗まれ、個人情報を紛失した。
ＵＳＢメモリには、担任児童３７名の各教科の試験結果等が記録されていた。
盗難にあった鞄は、約１か月後にＵＳＢメモリと一緒にショッピングセンター付近のゴミ置き場で発見された。

☆　なぜ、校長の許可を得なかったのでしょうか。もし、教諭Ａが校長の許可を求めていたら、その時、校長は「まっすぐ帰れよ。」「ＵＳＢメモリは肌身離さず持っていろよ。」と一声掛けてくれたはずです。
☆　最近の個人情報紛失事故の約７割は車上荒らしによるもので、帰宅途中に立ち寄った大衆浴場、ショッピングセンター、飲食店、保育園などの駐車場で発生しています。

◎　個人情報の取扱いや具体的な対応については、**「道立学校における個人情報の取り扱いについて」（平成１９年７月１２日付け教総第５６２号北海道教育委員会教育長通知）**により示されています。

【個人情報データの保管・管理の留意点】
・個人情報を取り扱うパソコンには、起動時にパスワードを入力するよう設定する。
・コンピュータウィルス対策ソフトを最新の状態にしておく。
・個人情報データは、暗号化やパスワードの設定を行う。
・個人情報を保存した記録媒体は、施錠のできる場所に保管する。
・原則として、個人情報を含むデータの複製は行わない。又、校外に持ち出さない。
・やむを得ず複製を必要とする場合や校外に持ち出す場合は、校長の許可を得る。
・個人情報の持ち出し状況を記録・管理するなど、学校におけるルールを明確にする。
・校外で利用するパソコンのセキュリティ対策についても学校全体で共通認識を形成する。
・個人情報データは、使用目的が終わった時点で消去等を行い、処分する。

《個人情報紛失の責任》

・　**車上荒らしなど**第三者による行為であっても、車内への放置など**適正な管理を行っていない場合は、管理責任が問われます。**
・　紛失した個人情報が後日発見されても、個人情報の流出の可能性は否定できません。
・　個人情報を紛失した場合は、原則として**懲戒処分（戒告）**の対象となります。

○　最近発生した事例

教諭Ｂは、前任校の生徒の成績等が記録されているパソコン及びＵＳＢメモリを鞄に入れ帰宅する途中、子供を迎えに保育園に立ち寄り、鞄を後部座席に置いたまま自家用車を駐車した際、車上荒らしに遇い、車内に置いてあった鞄を盗まれ個人情報を紛失した。

当該教諭は、前任校で育児休業中の２年４か月の間、個人情報が記録されているパソコン及びＵＳＢメモリを自宅に持ち帰り保管しており、復職した当日に新任校に持参したパソコン及びＵＳＢメモリを帰宅途中、車上荒らしに遇い紛失した。

事務職員Ｃは、個人情報の複製が禁止されているにもかかわらず個人情報をＵＳＢメモリに保存し、職員室で当該メモリを使用しパソコンで資料作成を行い退勤したが、メモリをパソコンに接続したまま退勤したものと思い、翌日、出勤後にパソコンを確認したところ接続されておらず、ＵＳＢメモリを紛失した。

当該職員は、個人情報を記録したＵＳＢメモリを日常的に自宅に持ち帰っており、当日もＵＳＢメモリをパソコンに接続したまま退勤したか、校外に持ち出したか分からない状況とであった。

☆　使用目的の終わった個人情報を消去することもなく長期間にわたり自宅で保管したり、個人情報を目的もなく日常的に自宅に持ち帰るなど、個人情報の適切な保管・管理に対する意識が欠如している事例です。

このような事態を踏まえ、今後は校長の許可なく個人情報を長期間にわたり持ち出し処分の対象となる者や、校外への持ち出しを常態化して処分の対象となる者については、より厳正に対処することとした。（平成２１年７月２２日付け教職第７２８号教職員課長通知）

もう一度、確認してください。

【チェックポイント】

- □　個人情報を取り扱うパソコンに起動時のパスワードが設定されているか。
- □　コンピュータウィルス対策ソフトは導入されているか、また、最新のウイルス定義ファイルに更新されているか。
- □　個人情報データに暗号化やパスワードの設定をしているか。
- □　個人情報を保存した記録媒体は、施錠できる場所に保管しているか。
- □　個人情報を含むデータの複製を行っていないか又、校外に持ち出していないか。
- □　やむを得ず複製を必要とする場合や校外に持ち出す場合は、校長の許可を得ているか。
- □　やむを得ず校外に持ち出す場合は、まっすぐ帰ることを心がけているか。
- □　車内等で一時的に保管する場合は、特に留意しているか。
- □　個人情報データは、使用目的が終わった時点で消去等を行い、処分しているか。

- **児童生徒、保護者は、学校を信頼して個人情報を預けているのです。**
- **不祥事を防ぐ最大の力は、教職員一人一人の自覚と努力です！**