

# 喜多方市立第二小学校個人情報保護規定

## 1 基本方針

- (1) 本校が所有する個人情報を含む情報資産を、盗難、紛失、コンピューターウイルス感染等による流失・漏洩の脅威から保護することを第一とする。
- (2) 業務上の利便性を確保しつつ、健全で安全な学校教育活動を支援するものである。
- (3) 校内における個人情報資産の重要性の理解促進と円滑なセキュリティ及び運用のための指針とする。
- (4) 適用範囲
  - ① 本校に勤務する校長、教頭、教諭、養護教諭、事務職員、常勤講師、非常勤講師、用務員、教育実習生等の本校児童の教育に携わる者（以下 本校職員）に対し適用されるものとする。

## 2 組織体制

- (1) 管理責任者
  - ① 個人情報の適正な安全管理及び保護を図るため、学校最高情報責任者「学校C I O」を学校長、統括責任者を教頭とする。
    - ア 学校C I Oは、本校の個人情報保護に関する権限及び責任をもつ。また、策定及び運用に関する最終決定権限をもつ。
    - イ 統括管理者は、本校において個人情報が適正に取り扱われていることを掌握し監督する。
- (2) 個人情報等保護管理委員会とその役割
  - (1) 本校の個人情報保護規定を作成し、運用、維持するために個人情報等保護管理委員会を設置する。個人情報等保護管理委員会は、教頭、教務主任、情報教育担当をもって構成するものとする。
    - ① 委員会は、4月と3月に個人情報保護に関する校内研修会を実施し、セキュリティ運用の確認や見直し等を行う。また、随時セキュリティ推進のための情報提供、環境改善を行うものとする。
    - ② 委員会はセキュリティの確保のために本校職員の役割・責任等を定め、本校職員のセキュリティ意識の向上を図る。
    - ③ セキュリティに関する事故が発生した場合、速やかに適切な処置が取られるよう、具体的な連絡体制を構築する。（個人情報流出への対応）

## 3 情報資産及び情報資産区分について

<定義>

- (1) 情報資産とは、本校が業務で扱う情報に関連するもので守るべき価値を持つものをいう。ここでは、コンピュータ及びネットワーク、電子媒体に記録されたデータ、印刷された文書類、ハードウェア、ソフトウェア等が含まれる。
- (2) 重要情報資産区分とは、本校が業務で扱う情報の中で個人情報が含まれている情報資産を区分Ⅰ、情報区分Ⅰ以外の情報を区分Ⅱとする。**※個人情報とは、生存する個人のもので、特定の個人を識別できる情報や組み合わせによって個人を識別できる情報とする**
  - ① 区分Ⅰの内容
    - i 形態は、紙、文書、電子データ、音声、映像等有形無形を問わない。

- 指導要録、生徒指導関係記録、出席簿、通知表、成績に関する表簿、学力テスト関係、進路調査等
- 児童名簿、緊急連絡網、
- ii 個人情報の適用範囲は、児童、保護者の他に、教職員、教育実習生等の本校で教育を行うもの者とする。

#### <情報資産の扱い>

- (3) 個人情報等保護管理委員会を中心に、学校内の全ての情報資産を洗い出し、それらに基づき情報資産目録を作成する。
- ① 情報資産目録には、資産名、管理者、記載内容、保管場所、保管状況、予想される脅威を明示し、それらに基づき資産評価を行う。
  - ② 資産評価ごとに対応策を考え、各管理者が責任をもって管理する。
  - ③ 情報資産目録は、定期的に見直すとともに、変更があった場合は、委員会が速やかに反映させる。

## 4 個人情報保護のための教職員の役割について

- (1) 本校職員は、個人情報保護のために以下のことを守らなければならない。
- ① 個人情報等保護管理委員会の定める役割分担、対策に従って個人情報の保護、安全管理に努める。
  - ② 必要に応じて情報セキュリティ研修を受け、本校の個人情報保護の向上に努める。
  - ③ 本校の個人情報を扱う外部委託業者に対して、必ず個人情報の安全が確認指されているか確認する。必要に応じて個人情報保護に関する契約を結ぶ。  
(例：学力テスト、スポーツテスト、卒業文集等)
  - ④ 本校で個人情報保護に関する事件、事故が起こった場合は、速やかに校長、教頭に詳細を報告し、指導を受けながら事件・事故の再発防止に取り組む。
  - ⑤ 本校を転出・退職した後も、守秘義務を守り、業務上知り得た個人情報の保護や安全管理に努める。

## 5 個人情報を含む紙・文書の取り扱いについて

### <作業の原則>

- (1) 作業中は、整理整頓に努め、決められた保管場所・保管方法を厳守する。

### <持ち出し時の盗難・紛失対策>

- (2) 原則として、個人情報を含む紙・文書を校外に持ち出すことを禁止する。ただし、以下の条件を満たす場合に限り、持ち出すことができる。
- ① 個人情報持ち出し簿に記入し、校長、または教頭の承諾を得る。
  - ② 持ち出す情報は、必要最低限にとどめ、必要のない情報を持ち出さない。
  - ③ 散逸しないよう、梱包の仕方を工夫している。(チャック付き鞆、ファイル化)
  - ④ 移動中、常に携行し、車内等に放置しない。
  - ⑤ 他が容易にアクセスする場所で作業しない。
- ※ 懇親会等の会合に参加する場合は、いかなる場合も持ち出し禁止とする。

### <不正アクセス>

- (3) 児童、保護者、業者等による盗み見、改ざん、複製等を防ぐために、他が容易にアクセスする場所での作業を避けなければならない。また、職員室や教室等で児童がアクセスできるような状態になった場合も、その都度、他の目に触れないよう配慮しなければ

ならない。

#### <廃棄方法>

- (4) 業務上不要になった個人情報を含む紙・文書は、以下の方法に従い、完全に復元できない方法で廃棄する。
- ① 少量ですぐに処分してかまわないものは、シュレッダーで処分する。
  - ② 処分する量が多く、シュレッダーで処分しきれないものは、個人情報等保護管理委員会が用意した廃棄ボックスに廃棄する。
  - ③ 3月の個人情報保護研修会時に一斉の廃棄作業を位置付け、年度末に処分する不要な紙・文書を廃棄する。
  - ④ 廃棄ボックスの管理は、個人情報等保護委員会が行い、安全な場所に設置する。また、確実な方法で廃棄する。

## 6 個人情報を含む電子データの取り扱いについて

#### <作業の原則>

- (1) 校内での作業は、業務用コンピュータで行い、情報はNAS（共有ファイル）内にて作成・保存し、業務目的の範囲内で利用すること。

#### <持ち出し時の盗難・紛失対策>

- (2) 原則として、個人情報を含む電子データを校外に持ち出すことを禁止する。ただし、以下の条件を満たす場合に限り、持ち出すことができる。
- ① 個人情報持ち出し記録簿に記入し、校長または教頭の承諾を得る。
  - ② 持ち出す情報は、必要最低限にとどめ、必要のない情報を持ち出さない。
  - ③ 情報資産を持ち出す場合は、必ずセキュリティが確保されたUSBメモリを使用し、手元から離さない。
  - ④ 記録媒体（USBメモリ、外付けHDD、FD、CD、DVD等）にデータを記録し、持ち出すことを禁止する。
  - ⑤ 暗号化で使用するパスワードは、第3者に推測されにくいものを使用し、他に漏れないように厳重に管理する。
  - ⑥ 返却時は、持ち出した情報資産がすべて揃っているかどうか確認すること。不足があることが分かった時は、直ちに学校長に報告すること。
- ※ 懇親会等の会合に参加する場合は、いかなる場合も持ち出し禁止とする。

#### <不正アクセス>

- (3) 自宅等で作業をする時は、コンピュータウィルス感染によるデータの流出、第3者による不正操作、データ改ざん、複製等を防ぐために、以下の対応策をとらねばならない。
- ① Windows Updateを行い、最新のセキュリティホール対策をとっている。
  - ② ウィルス対策ソフトを導入し、パターンファイルを最新の状態にしている。
  - ③ Winny等のファイル共有ソフトをインストールしない。
  - ④ 必要に応じてアプリケーションソフトのセキュリティアップデートを行う。
  - ⑤ 個人情報等保護委員会が認めたコンピュータ以外に電子データは保存しない。

#### <操作ミス、管理ミス>

- (4) パスワードを厳重に管理し、第3者の目に触れないように配慮する。
- (5) 原則として重要な個人情報をメールで送信しない。緊急な場合は、校長の了解を得て、

添付ファイルを暗号化するなどの注意を払い送信する。

#### <廃棄方法>

- (6) 業務上不要になった個人情報を含む電子データは、以下の方法に従い、完全に復元できない方法で削除する。
  - ① 処分してもかまわない電子データは、完全に復元できない方法で削除する。
  - ② 3月の研修会に一斉の削除作業を位置付け、委員会の指示に従って電子データを削除する。
  - ③ 転勤、退職等で本校の業務を離れる場合、業務上作成した個人情報を含む個人データは学校に帰属するものとし、NASに保存する。

### 7 ネットワークやソフトウェア等の運用管理について

- (1) 個人情報等保護委員会は、ネットワーク、サーバ、周辺機器が破壊されたり、不正操作や不正アクセスされたり、誤操作によるトラブルが生じないように管理する。
- (2) 個人情報等保護委員会は、サーバ等に保存されている重要な電子データが校外に流出・漏洩しないように厳重に管理する。
- (3) 個人情報等保護委員会は、業務用コンピュータで動作するソフトウェアを管理し、必要のないソフトウェアがインストールされないよう管理する。
- (4) 業務用として配布されているコンピュータの持ち出しは原則として認めない。

### 8 電子データ、コンピュータのアクセス制限について

#### <パスワードポリシー>

- (1) パスワードの秘密を保持し、メモ等が第3者の目に触れないよう、厳重に管理する。

#### <コンピュータ等のアクセス制限>

- (1) 業務用として認められたコンピュータ以外は、校内ネットワークに接続してはならない。

### 9 法令の遵守について

- (1) 本規定をよく理解した上で、これを遵守し本校のセキュリティの確保と個人情報の保護に努めなければならない。
- (2) 本規定は個人情報等保護委員会を中心に定期的に見直し、常に校内の実態に合ったものにしていく。
- (3) 本校職員は、上位法令である「喜多方市個人情報保護条例」「福島県個人情報保護条例」を理解し、遵守しなければならない。
- (4) 著作権、肖像権を理解し、これらを遵守しなければならない。

平成25年4月1日より運用