日置市立伊集院中学校情報セキュリティポリシー

日置市立伊集院中学校

1　基本方針

学校における情報資産（生徒，保護者，教職員などの個人情報及び学校運営上の重要な教育情報）の保護やインターネットの利用及び運営管理に関し，適切に管理・運用するための共通ルールを定め，組織的で継続的な対応を行なう。

2　適用対象者

本校に所属する教職員等とする。

3　適用範囲

（1）学校の情報資産及びネットワーク

（2）学校のネットワークに一時的に接続されたものや学校の情報資産を保持している機器（ＵＳＢメモリ，ＣＤ等）

（3）印刷物など二次的に生産されたもの

（4）生徒指導要録・家庭調査票・健康診断票・歯の検査表・個人指導カルテなどをはじめ，生徒・保護者・職員の個人情報の含まれる文書類

4　組織・体制

（1）校長は，すべての情報セキュリティに関する権限及び責任を負う。

（2）校務分掌又は委員会において情報セキュリティ担当者を置く。

（3）対象者は，本校の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。

（4）対象者は，異動・退職などの場合，知り得た情報を学校外で漏らしてはならない。

（5）年度当初に，情報セキュリティの研修会を行なう。

5　情報機器・ネットワーク管理

（1）情報セキュリティ担当者は，学校所有コンピュータのメンテナンスを随時行い，共有データのバックアップを定期的に行う。

（2）コンピュータ等の情報機器は，校長の許可なしには持ち出さない。

（3）校務で作成するデータについては，すべて校内サーバーに保存する。

（4）ネットワークに接続するコンピュータは，サポート対応のオペレーティングシステムのみとし，適宜セキュリティアップグレードを行う。

（5）インターネットの利用や電子メールの利用は，教育活動に限定する。

（6）生徒のインターネットを利用した情報発信は，教職員の指導の下におこなう。

（7）原則として校務は校務用のコンピュータを使用する。校務上必要で個人所有のコンピュータを学校に持ち込む場合には，必ず校長の許可を得る。（但し　校務に関するデータは，ＵＳＢメモリ等に保存し学校から持ち出さない。）

6　情報資産管理

（1）情報資産や記憶媒体は机上に放置せず，所定の場所に保管して管理する。

（2）情報資産のＵＳＢメモリ等による校外への持ち出しは原則として禁止する。やむを得ず持ち出す場合には,校長の許可を得るとともに,データにパスワードをかけるなどの必要な措置を講じ，紛失・盗難などによる情報漏洩を防止しなければならない。

（3）情報資産を破棄する場合には，データのフオーマットによる消去や粉砕等により，確実に処理する。

（4）次の各号のいずれかに該当する情報資産を機密情報とする。

ア　生徒に関わる個人情報

イ　漏えいした場合に、学校及び行政に対する信頼を著しく害するおそれのある情報資産

ウ　情報システムに係るパスワード及びシステム設定情報

エ　暗号化のための秘密鍵及び共有鍵

機密情報の取扱い方法

原則として機密情報に指定された情報は，指定された教職員用のフォルダにのみ保管する。印刷した書類は，鍵のかかる書庫・金庫に保管する。

各種取扱いについて具体的な遵守事項は次のとおりである。

取扱い方法	データ	書類	注意事項
校外へのメール	原則禁止		添付する場合も含む。 ※インターネットメールは第三者に読まれてしまう可能性がある。
FAX 送信		禁止	※誤送信による情報漏えいを防ぐため
送付 (郵便・宅配)	受領が確認できる方法で送付すること	受領が確認できる方法で送付すること	※届いていない場合に追跡できるようにするため
保管	校務サーバの指定したフォルダに保管すること	鍵付きの書庫・金庫に保管すること	個人機器のハードディスクに保管することは禁止する。
保存媒体への保存	学校所有の媒体に保存し，鍵付きの書庫・金庫に保管する。		個人所有の保存媒体への保管は禁止する。 ※プライベートなデータと分離して安全性を高める。
携行(校外)	管理職の許可を得た上，必要最低限の情報だけを携行すること	管理職の許可を得た上，必要最低限の情報だけを携行すること	データを携行する場合は，データの暗号化もしくはパスワードをかけて保存すること。パソコン自体を携行する場合も同様とする。
コピー	バックアップコピーを除き原則禁止	原則禁止	
廃棄処分	フォーマットによる消去や粉砕	シュレッダー処分	

7　運用

（1）管理職及び情報セキュリティ担当者は，本ポリシーが遵守されているか確認し，重大なポリシー違反が明らかになった場合は，迅速に対応する。

（2）緊急時の対応については，管理職に連絡・相談をする。また，情報セキュリティ担当者は，原因の特定，被害や影響範囲の把握，経過の記録などを行い，被害が拡大しないようにネットワークを停止し，業者へ連絡するなどの対応を行う。校長は教育委員会その他関係機関へ速やかに連絡する。

8　評価・見直し

本ポリシー及び情報セキュリティ対策の実施状況を定期的に検証し,実態との相違等を評価する。情報セキュリティの脆弱性が発見された場合は必要とされる対策を講じ，必要に応じて本ポリシーの見直し及び更新を行う。

【附則】　本ポリシーは，平成２４年１月２３日より施行する。