○情報セキュリティ

・概要

⑴　情報セキュリティとは、学校内でのインターネットやコンピュータを安心して使用し、大切な情報が外部に漏れたり、ウイルスに感染してデータが破壊又は流出したということなどがないように必要な対策をとることをいう。

⑵　学校に置ける情報セキュリティは、利用する教職員すべてが共通の知識を持ち、データの管理方法などのルールを策定し、その遵守を徹底する。

・個人情報の管理

⑴　個人情報が漏洩しないように校外への持ち出しはしない。

⑵　個人情報は決められた専用のサーバのみに保存し、クライアントＰＣやＵＳＢメモリ等に保存しない。アクセス許可により他の職員に見られないように設定したフォルダと共有して利用できるフォルダを正しく使い分けできるようにする。

⑶　ＩＤ及びパスワードの適切な管理を行う。

⑷　校務系システムと学習系システムは論理的又は物理的に分離し、児童生徒側から校務用データが見えないようにする。

⑸　児童生徒が利用する学習系システムには、個人情報を含む情報の格納は原則禁止とし、やむを得ず格納する場合には、暗号化等の保護措置を講じる。

・コンピュータウイルスへの対処

⑴　記録媒体を使用する際には、必ずウイルスチェックをすること。（ＬＡＮケーブルをつなぐ前に）

⑵　セキュリティソフトの更新をこまめに行う。

⑶　私有パソコンは原則校内に持ち込まない。

⑷　ウイルスに感染した場合は次のような手順で対処する。

①　ほかのＰＣに感染しないよう、ＬＡＮケーブルを抜く。（本来はウイルスチェックを行っているので必要ない）

②　管理職及び情報担当者に報告し、指示を受ける。

③　セキュリティソフトで再検索を行い、対処方法に従い、ウイルス本体の駆除と感染ファイルの削除を行なう。対処方法にレジストリの書き替えがあると明記してあるときは、保守業者に連絡し、確認をしてもらう。

④　情報管理機関（教育研修センター等）に報告する。（処理が完了しても再度ＬＡＮケーブルをつないだ際にウイルスログが報告されるため）

・情報機器等の管理

⑴　管理台帳などで管理をし、定期点検以外に破損や不具合がある場合、保守業者等に連絡をとる。

⑵　情報機器は定期的に確認し、盗難や紛失のないようにする。

⑶　不要になった機器等は、情報管理機関を通してのみ処分する。その他の記録媒体等を処分する場合も情報が復元できないように消去した上で廃棄処分する。

以　下　余　白