宇部市立小・中学校情報セキュリティ対策基準

第１章 総則

１　趣旨

この基準は、「宇部市立小・中学校情報セキュリティポリシー基本方針」（以下「基本方針」という。）に基づき、学校の情報資産の適切な管理運用及び保護に関し、必要な事項を定める。

２　定義

（１）個人情報　生存する個人に関する情報であってその情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの。他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。

（２）パソコン　スマートフォン・タブレット端末等の携帯デバイス（以下、「タブレット端末等」という。）を含む。

（３）この基準において、その他の用語の意義は、基本方針第３条に規定するところによる。

３　管理組織

この基準は、基本方針第５条から第１３条までに規定する情報セキュリティ管理体制に基づき運用する。

第２章 情報資産の管理

１　情報資産の分類

情報資産は、情報セキュリティの重要度に応じ、次に掲げる区分に分類するものとする。

区 分	分 類 基 準
重要度１	・漏えい又は改ざんされた場合、児童生徒、保護者の財産及びプライバシー等に重大な影響を及ぼす情報資産 ・漏えい又は改ざんされた場合、個人又は法人その他の団体の利益を害するなど、学校に対する信頼を害する恐れのある情報資産 ・法令又は条例等により守秘されるものと規定されている情報資産 ・情報システムに係るパスワード及び設定情報
重要度２	滅失又はき損した場合、その復元が困難となり、業務に重大な支障を来す恐れのある情報資産
重要度３	重要度１及び重要度２以外の情報資産

２　データ・記録媒体の管理

（１）　管理者の責務

管理者は、その所管する外部記録媒体（以下「媒体等」という。）について、次に掲げる事項を実施し、適切に管理しなければならない。

〔注〕外部記録媒体とは、パソコンから容易に取り外しが可能な記録媒体で、フロッピーディスク、ＣＤ、ＤＶＤ、ＵＳＢメモリー等の持ち運びが容易なものや、外付けハードディスクやＮＡＳ等の設置型のものをいう。

ア　外部記録媒体について、作成から廃棄に至るまでの経過を記録した外部記録媒体管理簿（様式第１号）を作成し、定期的にウイルスチェックを実施するとともに、その

管理状況を随時、点検すること。

イ　重要度１及び重要度２のデータが記録されている媒体等については、火災、水害、ほこり、湿度等の影響を可能な限り排除した施錠可能な場所に保管すること。また、施錠可能な場所での保管が困難な場合は、持ち出しができないように固定すること。

（２）　職員の遵守事項

職員は、記録媒体等の取扱いについて、次に掲げる事項を遵守しなければならない。

ア　業務以外の目的で記録媒体等を作成することを禁止する。

イ　個人所有のパソコンに、個人情報その他重要度１及び２の情報を保存することを禁止する。

ウ　バックアップなど、真に必要な場合を除き、記録媒体等を複製することを禁止する。

エ　記録媒体等を、学校外へ持ち出すことを禁止する。ただし、業務上やむを得ない場合は、あらかじめ持ち出し管理簿（様式第２号）に必要事項を記載し、管理者の承認を得ること。

オ　記録媒体等を廃棄する場合は、廃棄過程又は廃棄後において第三者に入手されないよう十分注意すること。また、廃棄後において、いかなる方法によっても内容を復元されないよう、あらかじめ物理的破壊によりデータを完全に消去しておくこと。

カ　ＵＳＢメモリーの使用は、業務上やむを得ない場合に限ることとし、使用する場合は、保存されたデータについてパスワード設定・暗号化処理を行うこと。

キ　外部からのデータの取り込みなど、学校で管理してない外部記録媒体を使用する場合は、必ずウイルスチェックを行うこと。

３　情報システムの管理

（１）　管理者の責務

管理者は、次に掲げる事項を実施し、適切に管理しなければならない。

①　アクセス管理

ア　パソコンには、ログイン時にパスワードの入力を必要とするよう設定すること。ただし、児童生徒用のタブレット端末等については、この限りではない。

イ　校務用パソコンを操作する職員をあらかじめ指定し、指定した職員にのみパスワードを通知すること。

ウ　情報システムにログインする際は、ＩＤ及びパスワードの入力を必要とするようサーバ及びパソコンに設定すること。

エ　情報システムを操作する職員をあらかじめ指定し、指定した職員にのみＩＤを付与すること。

オ　職員が異動、退職等により情報システムの操作権限を失った場合は、当該職員のＩＤ失効に係る手続を速やかに行うこと。

カ　ハブ等の通信機器の空ポートは、他者が容易にケーブルを差し込むことができないような対策を講じるとともに、ハブは外部から容易に発見できない場所に設置すること。

②　ネットワークの管理

ア　校務用端末と指導者用・学習者用端末とは、物理的または論理的に切り離し、相互にアクセスできないようにしなければならない。

イ　校務用ネットワーク・教育用ネットワークそれぞれについて端末、プリンタ、ハブ等の位置が分かるように学校内のネットワーク図を作成すること。また、ネットワークを変更した場合は、速やかに修正し常に最新の状態にすること。

ウ　無線によるネットワークに接続できるパソコン・機器は、宇部市教育委員会事務局または各学校が調達し、宇部市教育委員会事務局が利用を承認したパソコン・機器のみとする。

③　教育

ア　職員について適宜、情報モラルについて適切な意識啓発を行うこと。

イ　児童生徒の発達段階に応じて、情報モラルについて適切な指導計画・体制を整備すること。

（２）　職員の遵守事項

職員は、パソコンの取扱いについて、次に掲げる事項を遵守しなければならない。ただし、児童生徒の学習者用端末については別紙「学習者用端末利用規程」に従うものとし、本文中の規定と運用中の学習者用端末利用規程が相違する場合は、学習者用端末利用規程を優先するものとする。

① ソフトウェア

業務に必要のないソフトウェアを利用することを禁止する。

② パスワード

ア　パスワードを他人へ教示することを禁止する。

イ　パスワードを記載したメモ等を作成することを禁止する。

ウ　パスワードを設定する場合、次に掲げるものを禁止する。

・空白文字（何も入れない）
・職員番号
・生年月日
・電話番号
・連続した同一の文字・数字
・ID と同一の文字・数字

③ インターネット・メール

ア　業務以外の目的でインターネットを利用することを禁止する。

イ　個人所有のパソコンを宇部市地域イントラネット網に接続することを禁止する。

ウ　宇部市が付与するメールアドレス（***@ube-ygc.ed.jp）は、宇部市立小・中学校に勤務する職員のみが使用できるものとし、業務以外の目的で使用することを禁止する。ｙｓｎ２１メール(***@ysn21.jp)について、業務以外の目的で使用することを禁止する。

エ　重要度１及び重要度２のデータを含むファイルをメールに添付して送信すること

を禁止する。業務上やむを得ない場合は、パスワードを設定すること。

オ　差出人が不明又は不自然に添付されたファイルを開封することを禁止する。

④ クラウドサービス

ア　各校にて独自にクラウドサービスを利用する場合は、事前に統括責任者（教育長）へ申請し、承認を得なければならない。

イ　業務において、個人のアカウントで利用しているクラウドサービスへの接続を禁止する。

ウ　クラウドサービスごとに別途作成するクラウドサービス利用手順書を遵守すること。

エ　児童生徒の住所･生年月日･家庭環境･成績などの機微情報はクラウドサービスに保存してはならない。

⑤ パソコン

ア　個人所有のパソコンを校内で使用してはならない。ただし、業務上やむを得ない場合で、あらかじめ管理者（校長）の承認を得ているときはこの限りではない。

その場合には、使用者は、使用の１週間前までに、以下の事項を記載した申請書を管理者（校長）に提出し承認を得るとともに、必ず使用前にウィルス対策等のセキュリティ対策を講じなければならない。

(ア) 使用内容(使用端末規格、使用機能、使用ソフト、使用データ、使用方法等)

(イ) 使用期間

(ウ) 個人所有パソコンを使用しなければならない理由

(エ) 使用に際して講じるセキュリティ対策

イ　校務用端末および児童生徒用端末及びその端末が接続されたネットワークに個人所有のパソコンを接続することを禁止する。

ウ　パソコンを学校外へ持ち出すことを禁止する。ただし、業務上やむを得ない場合で、あらかじめ管理者（校長）の承認を得ているときはこの限りではない。

エ　ノート型パソコンは、退出時には火災、水害、湿度等の影響を可能な限り排除した施錠可能な棚等（外部から容易に発見できない場所）に収納すること。

オ　ディスプレイに表示されている内容が、職員以外の第三者に閲覧されることがないよう、パソコンの設置場所やディスプレイの向きについて必要な措置を講ずること。

カ　パソコンを廃棄する場合は、廃棄過程又は廃棄後において第三者に入手されないよう十分注意すること。また、廃棄後において、いかなる方法によっても内容を復元されないよう、あらかじめ物理的破壊又は専用ソフトによりデータを完全に消去しておくこと。

キ　パソコンやファイルサーバー等を共有する場合は、外部から閲覧できないようにアクセス制限を行うこと。

ク　ディスプレイには必ずスクリーンセーバーを設定し、解除する時もパスワードを設定すること。

第３章 事故等への対処

情報セキュリティに関する事故又は情報システムの障害（以下「事故等」という。）が発生した場合は、次のとおり対処するものとする。

（１） 報告

ア 職員は、事故等を発見した場合は、状況を把握し、速やかに管理者に報告しなければならない。

イ 管理者は、当該事故等が極めて重大なもので、在籍児童生徒、卒業児童生徒、保護者への影響が高いと判断した場合は、事故報告書（様式第３号）を作成し、統括責任者、副統括責任者、責任者に報告しなければならない。

（２） 対応措置

ア 管理者は、事故等の報告を受けた場合は、当該事故等による被害の拡大を最小限に防ぐため、速やかに必要な措置を講じなければならない。

イ 管理者は、事故等の原因を解明し、再発防止のための必要な措置を講じなければならない。

附則

施行 平成２４年４月１日

施行 平成２７年３月１日

施行 令和３年４月１日

施行 令和４年４月１日