

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つ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）校務用端末 宇部市教育委員会事務局が調達し、利用を承認した、教職員が利用する校務用の端末

（３）指導者用端末 宇部市教育委員会事務局が調達し、利用を承認した、教職員が利用する学習用の端末

（４）学習者用端末 宇部市教育委員会事務局が調達し、利用を承認した、児童生徒が利用する学習用の端末

（５）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「記録媒体等」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、端末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記録媒体等については、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、タブレット端末、記録媒体等及び個人のアカウントで利用しているクラウドサービス（以下、個人所有の端末等）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 所管する記録媒体等の使用は、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や、所管していない記録媒体等を使用する場合は、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されていることを確認し、適切に管理しなければならない。

① アクセス管理

ア 校務用端末、指導者用端末、学習者用端末には、起動時にパスワード等の入力が必要とするよう設定すること。ただし、児童用のタブレット端末等については、この限りではない。

イ 校務用端末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端末・機器は、校務用端末、指導者用端末、学習者用端末及び宇部市教育委員会事務局が特別に利用を承認した端末・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、校務用・指導者用・学習者用端末の取扱いについて、次に掲げる事項を遵守しなければならない。ただし、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

ア 業務に必要なのないソフトウェアを利用することを禁止する。

イ 不正にコピーした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

・その他容易に推測できるもの

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 個人所有の端末等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 (**@ubeygc.onmicrosoft.com) 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。

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 個人情報を提供するクラウドサービスを利用する場合は、事前に統括責任者へ申請し、承認を得なければならない。

イ 業務において、個人所有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。ただし、事前に統括責任者から承認されたサービスにおいては、この限りではない。

オ 職員は、校務及び学習で利用するクラウドサービスについては、次に掲げる事項を遵守しなければならない。

(ア)校務用アカウントを使用できる端末は、校務用端末のみとする。

(イ)校務系情報へのアクセスは、管理者から付与された校務用アカウントからのみとすること。

(ウ)学習用アカウントを使用できる端末は指導者用端末及び校務用端末とすること。

(エ)端末は、ログインした本人(または管理者等)以外からの操作を受けることのないようにパスワードを設定する等の管理をすること。

(オ)アカウントのパスワードは、本人(または管理者等)以外が知り得ることのないよう、厳格かつ適正に管理すること。

(カ)クラウドサービス上のデータは、適切なアクセス制限を施された状態を維持し、アクセス許可が与えられるべきでない者からのアクセスを不可とすること。

(キ)クラウドからダウンロードしたデータの取扱いについては、そのクラウドサービスにより為されていたセキュリティ対策が講じられていないと捉え、適切なセキュリティ対策を行うことに留意すること。

⑤ セキュリティ対策

ア 業務において、個人所有の端末等を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) 個人所有の端末等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、指導者用端末、学習者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端末等を接続することを禁止する。

ウ 校務用端末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、あらかじめ管理者の承認を得ているときはこの限りではない。

エ 校務用端末（デスクトップ型を除く）、指導者用端末、学習者用端末は、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に、端末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 端末を廃棄する場合は、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 ファイルサーバー等でデータを共有する場合は、外部からアクセスできないようにすること。

ク 離席時には、必ず画面ロック等を実施すること。

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

令和 4 年 4 月 1 日一部改訂

令和 5 年 4 月 1 日一部改訂

令和 6 年 4 月 1 日一部改訂