群馬大学共同教育学部附属小学校　情報セキュリティガイドライン

1　基本方針

学校における情報資産（教職員，児童，保護者の個人情報及び学校運営上の教育情報）を保護して適切に管理・運用するためのルールを定める。

2　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) 校務分掌の ICT 管理係を「情報セキュリティ委員長」とする。

(3) 学校内に，校長を責任者とする「情報セキュリティ委員会」を設置する。委員は，校長，教頭，教務主任，ICT 管理係とする。

(4) 情報セキュリティ委員会では，以下のことを実施する。

〇各ポリシーやガイドラインの検討・見直し

〇セキュリティに関する事件・事故の継続的な監視及び技術的な改善策

〇セキュリティを強化するための取組の提案・検討

(5) 情報セキュリティ委員会は，コンピュータやサーバ，周辺機器，ネットワーク等の設備及びシステムの変更について「情報管理関係マニュアル」を作成して管理する。

(6) 情報セキュリティ委員長は，ネットワークにおけるデータのセキュリティ確保や，無認可のアクセスからの保護を確実に行う。

(7) セキュリティに関する事件・事故が発生した場合に，群馬大学総合情報メディアセンターやその他関係諸機関と連携・協議しながら，早期に対応する。

3　情報セキュリティ対策

(1)ハードウェア

ア　教師用

(ァ)学校所持端末

〇学校所持端末は，使用しない時には，教員室または教科等準備室において保管する。

〇学校所持端末は，起動時にログインパスワードを求められるよう設定しておく。

〇学校所持端末のログインパスコードは，以下に挙げる条件を満たしていることを必須とする。(総務省 Web ページ(https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html)参照)

a. 名前などの個人情報からは推測できないこと

b. 類推しやすい並び方やその安易な組合せにしないこと

〇校務または授業で使用するコンピュータや学校所持端末のシステムを変更する場合は，情報セキュリティ委員長の許可を得る。

〇学校所有のコンピュータおよび周辺機器，情報機器，ソフトウェアパッケージは，指定場所から校長の許可なしに校外へ持ち出さない。持ち出す場合には，「個人情報持ち出し簿」に記入し，校長の許可を得る。

〇学校所持端末を校外に持ち出す際には，以下に挙げる条件を満たしていることを必須とする。

a.「個人情報持ち出し簿」に記入し，校長の許可を得ていること

b.業務上必要と認められるもの以外に利用しないこと

c.端末管理の都合上，学校外で利用した内容については大学で管理していること及び，その情報が管理上必要と認められる場合に利用されることがあることについて同意を得ていること

〇転出等に伴い，学校所持端末を学校に返却する際は，端末内のデータ及びアカウント情報を消去する。

〇端末内のデータ及びアカウント情報の消去は，使用していた個人が行い，その後 ICT 管理係が確認する。

〇転入等に伴い，学校所持端末を貸与される際は，前年度に転出した教職員が使用していた端末を引き継ぐ。

（ィ）教師個人の端末

〇教師個人の端末を業務に持ち込む際には，年度当初に，「個人所有情報端末使用許可申請書」に署名し，校長の許可を得ることとする。

〇教師個人の端末は，起動時にログインパスコードを求められるよう設定しておく。ログインパスコードは学校所持端末と同じ条件とする。

〇教師個人の端末には，業務に関わるデータを保存せず，データ保存にはクラウド，または個人支給 USB を利用する。クラウドは，全学認証アカウントを用いてログインできる GoogleDrive または OneDrive 及びロイロノートとする。

イ　児童用

〇保護者に対し，家庭の通信環境（Wi-Fi やテザリングなど）を使用し，フリーWi-Fi には接続しないことを周知する。

〇保護者に対し，端末管理の都合上，家庭で利用した内容や履歴については大学で管理していること及び，その情報が指導上必要と認められる場合に利用されることがあること を周知する。

〇保護者に対し，アプリのインストールやアンインストールをしないことを周知する。

〇児童用端末のトラブルに関する問い合わせ・相談先は，ICT 管理係が一括して受けることとする。

〇ICT 管理係は，トラブルの内容を情報セキュリティ委員会及び担当事業者に報告し，対応する。

・修理：ICT ハード管理係が，状況を把握した上で，修理を依頼する。

・破損：ICT ハード管理係が，状況を把握した上で，修理を依頼する。ただし，使用上問題ない程度の破損であれば，そのまま使用を続けることもできる。

・紛失：家庭内で端末を紛失した場合，保護者に，弁償していただくことを伝え，捜

索を依頼する。端末が見つかるまで，校内の予備端末を貸与する。

・盗難：保護者に，端末の盗難届を出していただくことを伝える。端末が見つかるまで，校内の予備端末を貸与する。

(2) ソフトウェア・ネットワーク

ア　ソフトウェア

〇校務または授業で使用するコンピュータにソフトウェアをインストールする場合は，情報セキュリティ委員長の許可を得る。

〇各教職員や児童がシステムで使用する ID やパスワードは，同一組織内で重複せず，かつ他人に推測されにくいものとする。

〇アカウント ID やパスワードの管理は，本人及び保護者が責任をもって行う。

〇アカウント ID やパスワードを忘れた場合には，速やかに ICT 管理係に報告し，新しいパスワードを設定する。

〇初期パスワードは ICT 管理係が設定し，アカウントと共に利用者に配付する。

〇初期パスワードは，初回利用時に変更する。

イ　インターネット利用

〇教職員のインターネットの利用や電子メールの利用については，教育活動に限定する。

〇以下のことを，インターネットを使用する際の禁止事項とし，教職員，児童及び保護者に周知する。

a.インターネットで発信する内容については，言語，表現方法，内容等，人権に関わる表現に考慮して発信しなければならない。

b.非合法的な情報や公序良俗に反する情報等，教育活動において望ましくない情報の受発信が行われないようにしなければならない。

c.インターネットに接続したコンピュータ等の機能，校内ネットワーク，あるいはインターネットに支障を与えてはならない。

d.インターネットを通して得られた情報については，その著作権，肖像権，知的所有権等の権利を侵害してはならない。

e.インターネットを通して，商用その他営利目的の活動をしてはならない。

f.個人・団体を誹謗・中傷する内容の情報を発信してはならない。

〇児童が学校ホームページ及び電子メール等で発信するデータや情報は，必ず事前に教師が確認をする。

ウ　校内ネットワーク

〇校内ネットワークについては，教職員用と児童用のネットワークを分割し，別々のパスワードを用いて使用する。

〇教職員が個人所有のコンピュータをネットワークに接続する際は，校長の許可を得る。

〇外部者には学校内のネットワークやサーバにアクセスさせない。どうしてもアクセスすることが必要な場合には，校長の許可を得る。

(3) 情報発信

ア　学校ホームページ

〇学校ホームページ上のデータの管理は，次の各項に定めることとする。

・学校ホームページへの公開内容については校長または教頭の承認を得るものとする。

・情報セキュリティ委員会は，学校ホームページを日常的に閲覧し点検する。公開にふさわしくない内容のページを発見した場合には，速やかに対処する。

・保護者や閲覧者等から掲載情報の内容について指摘を受けた場合には，情報セキュリティ委員会で協議したのち，適切な措置を講じることとする。

・学校ホームページから他ページへのリンクは，教育的効果を十分配慮したうえで設定するものとする。不適切な情報等が含まれると判断されたページへのリンクは設定しない。

・本規程を学校ホームページ上で必ず公開するものとする。

イ　学校インスタグラム

〇学校インスタグラム上のデータの管理は，次の各項に定めることとする。

・学校インスラグラムへの公開内容については，校長，教頭，教務主任の承認を得るものとする。

・情報セキュリティ委員会は，学校インスタグラムを日常的に閲覧し，点検する。公開にふさわしくない内容のページを発見した場合には，速やかに対処する。

・保護者や閲覧者などから掲載情報の内容について指摘を受けた場合には，情報セキュリティ委員会で協議をしたのち，適切な措置を講じることとする。

・児童の個人情報に十分配慮する。

・写真は縮尺を用いて，画質を落としてから使用する。

ウ　授業等動画配信

〇授業その他の教育活動をオンライン配信する場合には，児童の個人情報に十分配慮する。

〇授業その他の教育活動をオンライン配信する場合には，著作権の侵害に十分配慮しながら，著作権協会やその他の関係諸機関と相談をする。

エ　個人情報の保護

〇学校からの情報発信に備え，入学時に全家庭から，「個人情報の使用に関する確認書」で，個人情報使用の承諾を得る。その際，個人情報を発信する趣旨を十分に説明する。

〇インターネットで発信する，児童の個人情報の範囲は，次の各項に定めるものとする。

・氏名

原則として氏名は掲載しない。ただし，作品等に付す場合など，教育上必要がある場合に限り扱うことができるものとする。

・肖像(写真等)

生徒の写真については，教育上の必要に応じて，個人写真を扱うことができるものとする。その際，集合写真にしたり，氏名を同時に添えたりしないなど個人を特定

できないよう配慮するものとする。

・意見，主張等

児童の意見，考え，主張等については，教育上の効果が認められる場合において扱うことができるものとする。

・生活に関する情報

国籍，思想，信条に関する情報及び住所，電話番号，生年月日は，発信しないものとする。

・年齢，性別，趣味，特技等の個人の情報については，教育上の効果や必要性が認められる場合においてのみ扱うことができるものとする。

(4) 校務に関わる情報の取り扱い

〇児童に関する記録，名簿，成績等のデータをコピー又は印刷して，学校外に持ち出すことは原則として禁止する。やむを得ず必要となった場合は，個人情報持ち出し簿に記入し，校長の許可を得る。

〇児童の成績は，専用の USB メモリーで管理し，成績処理作業は必ず教員室で行う。なお，成績に関わるデータは PDF で保存しないこととする。

〇受信した個人情報を修正・加工，再発信しないこととする。

〇校務に関わる情報の分類及び取扱は，別紙１及び２に示す。

4　教職員，児童，保護者への周知

(1) ハードウェア

タブレット端末使用上の約束

タブレット端末の貸与についての承諾書

(2) ソフトウェア・ネットワーク

インターネット利用上の注意

(3) 情報発信

個人情報の使用に関する確認書

(4) 情報モラル

情報モラル教室実施（5 学年：7 月）

5　情報セキュリティガイドラインの運用

(1) 教職員は，本ガイドラインの内容を理解し，遵守する。

(2) 情報セキュリティ委員会は，本ガイドラインが適切に遵守されているか確認する。また，重大なガイドライン違反が明らかになった場合は，迅速に対処する。

(3) セキュリティの事件・事故が発生した場合，情報セキュリティ委員長は，原因の特定，被害や影響の範囲の把握，経過の記録などを行い，被害が拡大しないようネットワークを停止し，速やかに校長に連絡する。

(4) セキュリティの事件・事故が発生した場合，校長は群馬大学やその他関係機関へ速やかに連絡する。

6　監査・評価・見直し

(1) 情報セキュリティ委員会は，本ガイドラインに定める事項について，常に実態との相違等を監査し評価を行う。

(2) 情報セキュリティ監査における評価及び情報セキュリティを取り巻く状況の変化をふまえ，必要に応じ本ガイドラインの見直し及び更新を行う。

7　関係諸機関連絡先

〇群馬大学総合情報メディアセンター【校内ネットワーク関係】（027-220-7188）

〇電通システム【校内サーバ関係】（027-361-3211）

〇EDUCOM【C4th 関係】（00777-81056）

〇滋野堤水堂【教育機器関係】（027-243-7116）

令和３年４月　１日策定
令和５年４月２８日改訂
令和６年５月　１日改訂
令和７年４月　４日改訂

別紙１

情報資産の分類					情報資産		
重要性分類	定義	機密性	完全性	可用性	校務系	学習系	公開系
Ⅰ	セキュリティ侵害が教職員又は児童生徒の生命，財産，プライバシー等へ重大な影響を及ぼす	3	2B	2B	・指導要録原本 ・教職員の人事情報 ・入学者選抜問題，実施要項 ・教育情報システム仕様書		
Ⅱ	セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす	2B	2B	2B	○学籍関係 ・卒業証書授与台帳 ・転退学受付（整理）簿 ・転入学受付（整理）簿 ・休学・退学願等受付（整理）簿 ・教科用図書給与児童名簿 ・要・準要保護児童認定台帳 ○成績関係 ・通知票 ・進級・卒業認定資料 ・テストの答案用紙（児童が記入済みのもの） ・テストの素点表 ・成績に関わる個票等 ○指導関係 ・事件事故報告書 ・生徒指導の記録 ・児童個別・集合写真 ・教育相談の記録 ・個別の支援計画 ・各種面談記録 ・教務手帳 ○進路関係 ・調査書，推薦書 ・入学願書 ・卒業生名簿 ・進路希望調査 ・卒業・進級認定会議資料 ○健康関係 ・健康診断票 ・歯の検査票 ・心臓管理等医療情報 ・健康保険等被保険者証の写 ・要管理児童一覧 ○名簿等 ・児童名簿 ・緊急時連絡票 ・家庭調査票 ・ＰＴＡ各委員会名簿 ○教職員に関する情報 ・電話番号，住所，メールアドレス等基本的な情報 ・病歴，心身の状況，収入等の個人情報 ・情報システムや情報端末のログインＩＤ/ＰＷ管理台帳	○児童に割り当てた情報 ・情報システムや情報端末のログインＩＤ/ＰＷ管理台帳	
Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす	2A	2A	2A	○児童の氏名 ・出席簿 ・座席表 ・クラブ，委員会，異年齢活動の名簿 ○学校運営関係 ・卒業アルバム ・学校行事等の児童写真	○学校運営関係 ・授業用教材 ・教材研究資料 ・児童用配付プリント ○児童の学習系情報 ・児童の学習記録（ワークシート，作品等） ・学習活動の記録（動画や写真等）	
Ⅳ	影響をほとんど及ぼさない	Ⅰ	Ⅰ	Ⅰ			○学校運営関係 ・学校要覧 ・学校紹介パンフレット ・学校行事実施計画 ・各種届様式 ・学校，学年，学級通信 ・学校ＨＰ掲載情報 ・学校行事のしおり ○学校生活の記録 ・学校行事等の児童写真・動画・作品等（名前が分からないもの）

別紙２

情報資産の分類					情報資産の取扱								
重要性分類	定義	機密性	完全性	可用性	複製・配付	外部への持ち出し制限＊	端末制限	外部への情報の送信＊＊	情報資産の運搬＊＊＊	外部での情報処理＊＊＊＊	使用する電磁記録媒体	情報資産の保管	情報資産の破棄
Ⅰ	セキュリティ侵害が教職員又は児童生徒の生命，財産，プライバシー等へ重大な影響を及ぼす	3	2B	2B	必要以上の複製及び配付禁止	本ガイドラインに準拠していることを確認した上で業務遂行上必要な場合には，情報セキュリティ管理者の判断で持ち出しを可	支給以外の端末での作業の原則禁止	限定されたアクセスの措置がとられていること＊＊＊＊＊	鍵付きケースへの格納	禁止	施錠可能な場所への保管	・耐火，耐熱，耐水，耐湿を講じた施錠可能な場所に保管（電子データの場合もこれらの対策に準じたサーバに保管） ・情報資産を格納するサーバのバックアップ ・６か月以上のログ保管 ・サーバの冗長化（推奨事項） ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁記録媒体の持ち込み禁止	電子記録媒体の初期化，復元できないようにして廃棄
Ⅱ	セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす	2B	2B	2B	同上	同上		同上	同上	安全管理措置の規定が必要	同上	同上	同上
Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす	2A	2A	2A	同上	情報セキュリティ管理者の包括的承認で可		同上	同上	同上	同上	・耐火，耐熱，耐水，耐湿を講じた施錠可能な場所に保管（電子データの場合もこれらの対策に準じたサーバに保管） ・情報資産を格納するサーバのバックアップ（推奨事項） ・一定期間以上のログ保管 ・サーバーハードディスクの冗長化（推奨事項） ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁記録媒体の持ち込み禁止	同上
Ⅳ	影響をほとんど及ぼさない	1	1	1									

＊：外部への持ち出しとは，大学や学校が構築・管理している環境（本ガイドラインが適用されているクラウドサービスを含む環境）の外に情報資産を持ち出すことを示す。
＊＊：情報の外部への送信とは，情報システムを構成するネットワーク，端末，サーバの閉じた領域の外側に，情報資産をオンラインで持ち出すことを示す。
＊＊＊：情報資産の運搬とは，USBメモリやハードディスク等の電磁的記録媒体を介して情報資産を運搬する場合を示す。
＊＊＊＊：外部での情報処理とは，大学や学校が構築・管理している環境（本ガイドラインが適用されているクラウドサービスを含む環境）の外において情報資産を管理・電算処理することを示す。
＊＊＊＊＊：限定されたアクセスの措置とは，適切かつ限定的な利用を前提とし，外部に送信される際に適切なアクセス制限を講じることを指す。