

令和5年 1月 1日作成
令和8年 4月30日改定

1 趣旨

この実施手順は、吹田市教育情報セキュリティポリシー（以下「教育情報セキュリティポリシー」という。）に基づき、校内で教育情報システムを利用するにあたって、適正な管理・運用、個人情報保護を図るため、教職員等が遵守すべき具体的な事項を定めるものである。

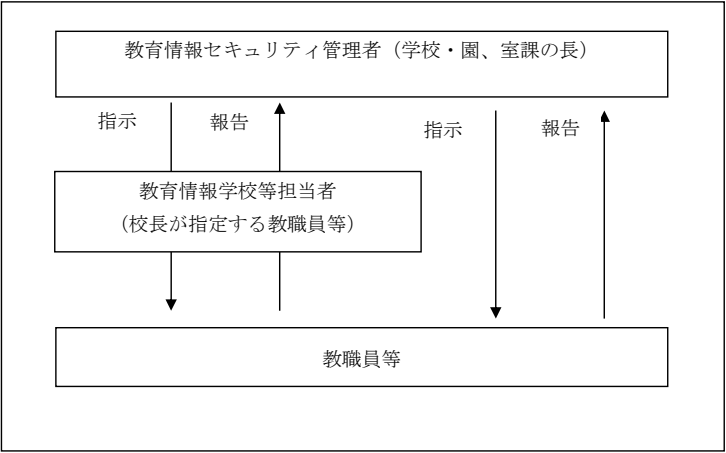
教職員等は、この実施手順を遵守し、情報セキュリティを確保しなければならない。

2 用語説明

用語	定義
校務系情報	学校が保有する情報資産のうち、それらの情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報
校務外部接続系情報	ネットワーク分離による対策を講じたシステム構成において、インターネット接続を前提として、校務で利用される情報
学習系情報	学校等が保有する情報資産のうち、それらの情報を学校における教育活動において活用することを想定しており、かつ、当該情報に教職員及び児童・生徒がアクセスすることが想定されている情報
校務用端末	校務系情報にアクセス可能な端末
校務外部接続用端末	ネットワーク分離による対策を講じたシステム構成において、校務外部接続系情報にアクセス可能な端末
学習者用端末	学習系情報にアクセス可能な端末で、児童生徒が利用する端末
指導者用端末	学習系情報にアクセス可能な端末で、教員のみが利用可能な端末
校務系システム	校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム及び、校務系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
校務外部接続系システム	ネットワーク分離による対策を講じたシステム構成において、校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ（CMS）及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム
学習系システム	学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム及び、学習系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
教育情報システム	校務系システム、校務外部接続系システム及び学習系システムを合わせた総称
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	ネットワーク分離による対策を講じたシステム構成において、校務外部接続系情報を取り扱うサーバ
学習系サーバ	学習系情報を取り扱うサーバ

3 校内組織体制

校内の組織体制の図を以下に示す。



4 情報資産の分類と管理方法

（1） 情報資産の分類

本市における情報資産は機密性、完全性及び可用性の3つの側観点から影響度を評価し、次のとおり4段階の重要性分類を行い、必要に応じて取扱い制限を行うものとする。

重要性分類	
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。
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。（Iを除く）
III	セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼす。（II以上を除く）
IV	セキュリティ侵害が学校事務及び教育活動の実施に影響をほとんど及ぼさない。（III以上を除く）

情報資産の分類		情報資産の例（アクセスする主体）		
重要性分類	定義	教職員等・教育委員会	教職員等・教育委員会・児童生徒・保護者	不特定多数
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。	業務に係る特定の教職員等・教育委員会のみがアクセスすることが想定される情報 ○情報システムの設計に関する情報 ・教育情報システム設計書、設定書 ○学校運営に関する情報	業務に係る特定の教職員等・教育委員会に加えて、児童生徒又はその保護者がアクセスする場合、児童生徒本人の情報のみにアクセスすることが想定される、要配慮個人情報等を含む情報 ○健康に関する情報（医	

		・入学者選抜問題 ・指導要録原本 ・教職員の人事記録 ○健康に関する情報（医師等による指導、診療、調剤の事実等要配慮個人情報を含むもの） ○指導に関する情報（犯罪の経歴、犯罪により害を被った事実、少年法に関する事項等要配慮個人情報を含むもの） ○その他要配慮個人情報を含む情報 等	師等による指導、診療、調剤の事実等要配慮個人情報を含むもの） ・健康診断票 ○その他要配慮個人情報を含む情報 等	
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。（Ⅰを除く）	業務に係る教職員等・教育委員会のみがアクセスすることが想定される情報 ○情報システムの運用に関する情報 ・システムログイン ID 管理台帳 ・端末ログイン ID 管理台帳 ○学校運営に関する情報（Ⅰを除くもの） ・教職員および児童生徒の生活歴、電話番号、メールアドレス、住所、生年月日、性別等の基本情報を含むもの ○健康に関する情報（医師等による指導、診療、調剤の事実等要配慮個人情報を含むもの） ・養護教諭、スクールカウンセラー等による記録 ○指導に関する情報（Ⅰを除くもの） ・個別指導計画 ・生徒指導に関する記録	業務に係る教職員等・教育委員会に加えて、児童生徒又はその保護者がアクセスする場合、児童生徒本人の情報のみにアクセスすることが想定される、要配慮個人情報等を含まない情報 ○成績に関する情報 ・通知表 ・定期考査、テスト等の採点結果 ○健康に関する情報（医師等による指導、診療、調剤の事実等要配慮個人情報を含むもの）等	—

		・家庭訪問や個別面談に関する記録 ○成績に関する情報 ・進級、卒業認定資料 ○進路に関する情報 ・進路希望調査 ・入学者選抜に関する表簿（願書等） ・調査書 ・推薦書 ・卒業生進路先情報 ○学籍に関する情報 ・転退学、転入学、就学、休学等に関する情報 ・教科用図書の給付に関する情報 ○児童生徒の氏名 ・児童生徒名簿、児童生徒住所録 ・保護者緊急連絡網 ・職員緊急連絡網、職員住所録 等		
Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼす。（Ⅱ以上を除く）	教職員等全員・教育委員会がアクセスすることが想定される情報 ○学校運営に関する情報（職員室等で日常的に運用するもので、Ⅱ以上を除くもの） ・職員会議資料 ○児童生徒の氏名・所属等に関する情報（教室等で日常的に運用するもので、Ⅱ以上を除くもの） ・出席簿 等	教職員等全員・教育委員会に加えて、児童生徒及び保護者がアクセスすることが想定される情報 ○児童生徒の氏名・所属等に関する情報 ・座席表 ・児童生徒委員会名簿 ○学校運営に関する情報 ・卒業アルバム ・児童生徒の個人写真、集合写真、学校行事等の児童生徒の写真 ○学習活動の中で生成される情報 ・児童生徒の学習記録（確認テスト、ワークシート、レポート、作品、	—

			日常的な簡易な健康観察等) ・学習活動の記録(動画、写真等) ○学習指導に関する情報 ・授業用教材、児童生徒用配布プリント 等	
IV	セキュリティ侵害が学校事務及び教育活動の実施に影響をほとんど及ぼさない。(Ⅲ以上を除く)	教職員等全員・教育委員会がアクセスすることが想定される、Ⅲ以上を除く情報	教職員等全員・教育委員会に加えて、児童生徒及び保護者がアクセスすることが想定される、Ⅲ以上を除く情報 ○学校運営に関する情報(広報等のため活用するもの) ・学校、学園要覧 ・学校紹介パンフレット ・学校、学園ホームページ掲載情報 ○学習活動で生成される情報(保護者の同意等を得て広報等のため活用するもの) 等	

(2) 情報資産の管理

ア 教育情報セキュリティ管理者(学校・園、室課の長)は、標準情報資産台帳に基づき、所管する情報資産を確認し、不足内容を補完した所管向け情報資産台帳(以下「台帳」という。)を整備しなければならない。

イ 情報資産の管理(取扱い)

教職員等は、保管している情報資産について、以下の表に示されている取扱制限に従って、取り扱わなければならない。また、情報資産を複製した場合には、複製した情報資産も、同様に取り扱わなければならない。

情報資産の分類		情報資産の管理（取扱い）										
		学校外への持ち出し						複製・ 配付	端末制限	端末への 保存	電磁的記録 媒体の保管	電磁的記録 媒体の廃棄
重要性 分類	定義	禁止	制限	電子メール での送信	運搬	自宅パソコン での情報 資産処理	持出簿への 記録					
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。	児童生徒の転校等に伴う外部への情報移動の特別な理由を除いて禁止	外部連携が必要な場合に限り教育情報セキュリティ管理者（学校・園、室課の長）の許可で持ち出しを可/外部持ち出しルールに限定されたアクセスの措置設定(アクセス制限や暗号化)機能を有する場合には、有効にしなければならない。	暗号化、パスワード設定を行う	禁止	禁止	必要	必要以上の複製及び配布禁止	校務用端末以外の端末での作業の原則禁止	禁止	耐火、耐熱、耐水、耐湿を講じた施設可能な場所に保管/保管場所への必要以上の電磁的記録媒体の持ち込み禁止/指定された場所に保管	情報資産の物理的な破壊、初期化、紙媒体の場合は裁断、溶解など、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。（Iを除く）	同上	同上	同上	同上	同上	同上	同上	同上（※）	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影響を及ぼす。（II以上を除く）	教育情報セキュリティ管理者（学校・園、室課の長）の許可で持ち出しを可とする。	同上/但し、やむを得ない場合、教育情報セキュリティ管理者（学校・園、室課の長）の許可で可	同上	同上	同上	同上	同上	支給以外の端末での作業の原則禁止	授業等で使用する場合、一時的に保存可	指定された場所に保管	同上
IV	セキュリティ侵害が学校事務及び教育活動の実施に影響をほとんど及ぼさない。（III以上を除く）	同上	教育情報セキュリティ管理者（学校・園、室課の長）の確認のもと可	特になし	教育情報セキュリティ管理者（学校・園、室課の長）の許可で可	教育情報セキュリティ管理者（学校・園、室課の長）の許可で可	特になし	同上	同上	同上	特になし	特になし

(※) 児童生徒及び保護者がアクセスすることが想定される情報は学習用端末でのアクセスを許可するが、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等によるユーザ認証を行うこと

ウ 情報資産の作成

- (ア) 教職員等は、業務上必要のない情報資産を作成してはならない。業務とは、以下の内容を示す。
- a 学習指導要領に基づく児童・生徒の指導における使用。
 - b 情報通信機器の積極的活用を推進するための研修に関すること。
 - c 教育方法・内容の改善及び充実に関すること。
 - d 教育計画に基づいた学校管理に関すること。
 - e その他、教育情報セキュリティ管理者（学校・園、室課の長）に許可を得たこと。

(イ) 情報資産を新規作成する教職員等は、(2)イの表に基づき、取り扱わなければならない。

(ウ) 情報資産を新規作成する教職員等は、作成途上の情報資産についても、紛失や流出等をさせてはならない。また、情報資産の作成途上で不要になった場合は、当該情報資産を消去しなければならない。

エ 情報資産の入手

- (ア) 教職員等は、自校の教職員等から情報資産を入手した場合は、重要性分類に基づいた取扱いをしなければならない。
- (イ) 学校外の者が作成した情報資産を入手した教職員等は、(2)イの表に基づき、当該情報資産を取り扱わなければならない。
- (ウ) 情報資産を入手した教職員等は、入手した情報資産の重要性分類が不明な場合、教育情報セキュリティ管理者（学校・園、室課の長）に判断を仰がなければならない。

オ 情報資産の利用

- (ア) 情報資産を利用する教職員等は、業務以外の目的に情報資産を利用してはならない。
- (イ) 情報資産を利用する教職員等は、情報資産の重要性分類に応じ、取扱いをしなければならない。
- (ウ) 情報資産を利用する教職員等は、電磁的記録媒体に情報資産の重要性分類が異なる情報資産が複数記録されている場合、記録されている情報資産のうち重要性分類が最も高いものの分類に従って、電磁的記録媒体を取り扱わなければならない。

カ 情報資産の保管

- (ア) 教職員等は、情報資産の重要性分類に従って、情報資産を保管しなければならない。
- (イ) 教職員等は、情報資産を記録した電磁的記録媒体を長期保管する場合は、情報資産が改ざんされないように保管しなければならない。
- (ウ) 教職員等は、重要性分類Ⅰ、Ⅱ又はⅢの情報を記録した電磁的記録媒体を保管する場合、校長室や指導要録を保管している金庫に、必要に応じて保管しなければならない。
- (エ) 教職員等は、教育情報セキュリティ管理者（学校・園、室課の長）が指定した保管先のみ情報資産を保管しなければならない。
- (オ) 教職員等は、児童生徒が生成する学習系情報の保管先について児童生徒に指示し、それ以外の場所に保管しないよう指導しなければならない。
- (カ) 教職員等は、児童生徒が生成する学習系情報の保管先について児童生徒に指示し、それ以外の場所に保管しないよう指導しなければならない。

キ 電子メール、外部ストレージサービスによる情報の送信

- (ア) 重要性分類Ⅰ、Ⅱ又はⅢの情報を外部へ送信する場合は、教育情報セキュリティ管理者（学校・園、室課の長）の許可を得たうえで、限定されたアクセスの措置設定（アクセス制限や暗号化）を行わなければならない。
- (イ) 利用する電子メール、外部ストレージサービスは教育委員会又は学校から提供される公式サービスのみを利用し、私的に契約したサービスを利用してはならない。

ク FAXによる情報の送信

FAXによる情報の送信は、限定されたアクセスの措置（アクセス制限や暗号化）が不可能であること、誤送信のリスクがあることに鑑み、送信相手がFAX受信を指定してきた場合にのみ利用すること。

ケ 電磁的記録媒体の運搬

- (ア) 重要性分類Ⅰ又はⅡの情報資産の学校外への運搬は、禁止する。
- (イ) 重要性分類Ⅲ又はⅣの情報資産を学校外へ運搬するときは、必要に応じ鍵付きのケース等に格納し、暗号化またはパスワードの設定を行う等、情報資産の不正利用を防止するための措置を実施しなければならない。
- (ウ) 重要性分類Ⅲ又はⅣの情報資産（複製を含む。）の保管場所からの移動や学校外への持ち出し業務が必要となったときは、教育情報セキュリティ管理者（学校・園、室課の長）の許可を得なければならない。
- (エ) 教育委員会又は学校から支給された公的な媒体以外は使用してはならない。
- (オ) 暗号化機能付きの媒体を利用し、確実に暗号化機能を有効にしなければならない。
- (カ) 車両等により重要性分類Ⅲ以上の情報資産を運搬する場合は、必要に応じ暗号化又はパスワードの設定を行う等の安全管理措置を講じ、宛名・差出名を明記して、厳重に封印しなければならない。

コ 情報資産の提供・公表

- (ア) 重要性分類Ⅰの情報資産は、外部に提供できない。
- (イ) 重要性分類Ⅱ又はⅢの情報資産を外部に提供する時は、必要に応じ暗号化又はパスワードの設定を行わなければならない。
- (ウ) 重要性分類Ⅱ又はⅢの情報資産を外部に提供する時は、教育情報セキュリティ管理者（学校・園、室課の長）に許可を得なければならない。
- (エ) 保護者や地域に公開する情報資産について、勝手に書き換えられないように保存しなければならない。
- (オ) 教育情報セキュリティ管理者（学校・園、室課の長）は、公開する情報が正しい内容であることを事前に確認し、誤公開を防がなければならない。
- (カ) 教育情報セキュリティ管理者（学校・園、室課の長）は、住民に公開する情報資産について、改ざんや消去されないように定期的に確認しなければならない。

サ 電磁的記録媒体の廃棄

- (ア) 重要性分類Ⅰ、Ⅱ又はⅢの情報を記録している電磁的記録媒体の廃棄を行う教職員等は、不要になった場合、電磁的記録媒体を物理的に破壊する等、情報資産が復元されないための適切な措置を施したうえで廃棄しなければならない。
- (イ) 重要性分類Ⅰ、Ⅱ又はⅢの情報を記録している電磁的記録媒体の廃棄を行う教職員等は、行った処理について、日時、担当者及び処理内容を記録しなければならない。
- (ウ) 重要性分類Ⅰ、Ⅱ又はⅢの情報を記録している電磁的記録媒体の廃棄を行う教職員等は、

教育情報セキュリティ管理者（学校・園、室課の長）の許可を得なければならない。

（エ） 教育情報セキュリティ管理者（学校・園、室課の長）は、廃棄処理を外部に委託する場合は、学校の外に委託業者が持ち出す行為に教職員等が立ち合うように指示し、誤廃棄を予防しなければならない。

（３） 教職員等の情報セキュリティ意識醸成

ア 教育情報セキュリティ管理者（学校・園、室課の長）は、教職員等に対して、日頃から情報セキュリティに関する話題を積極的に提供し、情報セキュリティ研修を受講させるなど、積極的にセキュリティ認識の向上を図らなければならない。

イ 教育情報セキュリティ管理者（学校・園、室課の長）は、校内でセキュリティ事故につながりかねないヒヤリ・ハット事案を抑止するために、教職員等が事案を発見した際に、ただちに対処し、速やかに報告が上がるよう、教職員等に対する情報セキュリティ意識の醸成と風通しのよい関係性維持に努めなければならない。

ウ 教育情報セキュリティ管理者（学校・園、室課の長）は、教職員等が常に教育情報セキュリティポリシー及び実施手順を閲覧・確認できるよう配慮しなければならない。

エ 教育情報セキュリティ管理者（学校・園、室課の長）は、新規採用教職員等及び他自治体から本市に新規赴任した教職員等、及び非常勤及び臨時の教職員に対し、教育情報セキュリティポリシー等遵守すべき内容を理解・浸透するように指導を行わなければならない。

（４） 執務上での管理

ア 執務室にて教職員等が不在となる場合には、執務室を施錠しなければならない。

イ 教職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は教育情報セキュリティ管理者（学校・園、室課の長）の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

ウ 業務終了後と外出時には、電源を落とさなければならない。

エ 認証に用いる IC カード等を、教職員等間で共有してはならない。

（５） 情報資産の管理方法に関する例外措置①（流出した際の影響が軽微な個人情報が含まれる重要性分類Ⅲの情報資産）

ア 定義

教育活動を撮影した動画、静止画、児童生徒が学習活動によって作成した作品。但し、評価対象にするため改ざん等が行われてはならない情報を除く。これらの情報は、万が一、セキュリティ侵害により流出したとしても、「社会的差別の被害要因」「いじめ等の人間関係に影響を及ぼしうる原因」とはならないため、影響が軽微であると判断されるもの。

イ 学習系サーバにおける取扱い

前項「ア 定義」にて定義される個人情報が含まれる情報資産について、以下に運用方法を定め、それに従って取り扱う場合に限り、学習系サーバで取扱うことを可能とする。

（ア） 影響が軽微な個人情報が含まれる動画や静止画などの撮影したものを教育活動で使用するのをあらかじめ年度当初に、保護者に周知する。その使用にあたって配慮が必要な場合は申し出てもらう。

（イ） 動画、静止画の撮影は、名札をあらかじめ外すなど個人が特定されないよう配慮する。

（ウ） 影響が軽微な個人情報が含まれるデータがその利用目的を達成もしくは利用目的自体がなくなり、利用する必要がなくなったときは、速やかに削除する。

ウ オンライン会議システムにおける取扱い

前項「ア 定義」にて定義される個人情報が含まれる情報資産について、教育委員会が指定する録画機能が使用できないオンライン会議システムにて撮影し利用することを可能とする。

（６） 情報資産の管理方法に関する例外措置②（専用ソフトを使用した試験問題等の作成）

ア 専用ソフトで作成した試験問題等の取扱い

学校で購入した専用ソフトを使用して、試験問題等を作成する場合、教育情報セキュリティ管理者（学校・園、室課の長）の許可の下、当該作成データについては、学習系サーバで取り扱うことを可能とする。但し、データ保存の際は、パスワード設定などの暗号化措置を施すこと。

５ 物理的セキュリティ

（１） 校務用端末の管理

ア 端末機器の利用に際し、ログインや認証を必要とするように設定すること。なお、本端末は重要情報である校務系情報にアクセスを行う端末のため、ログイン時の認証はよりセキュリティが高い多要素認証（生体認証）を行うように設定すること。

イ 盗難防止のため、ワイヤーによる固定や施錠可能な保管庫又は引き出し等への保管の対策を行うこと。

ウ 本端末が盗難された場合、又はリース満了や故障等により端末の返却・廃棄となった場合、ハードディスク等より重要情報の漏えいが発生しない様に暗号化対策を講じること。

（２） 校務用端末（共有用）の管理

ア 端末機器の利用に際し、ログインや認証を必要とするように設定すること。なお、本端末は重要情報である校務系情報にアクセスを行う端末のため、ログイン時の認証はよりセキュリティが高い多要素認証（生体認証）を行うように設定すること。

イ 盗難防止のため、ワイヤーによる固定等対策を行うこと。

ウ 本端末が盗難された場合、又はリース満了や故障等により端末の返却・廃棄となった場合、ハードディスク等より重要情報の漏えいが発生しない様に暗号化対策を講じること。

（３） 事務なび端末の管理

本端末の所管課（情報政策室）の指示に基づき、必要な対策を実施すること。

（４） 授業・研修用端末の管理

ア 端末機器の利用に際し、ログインや認証を必要とするように設定すること。

イ 盗難防止のため、施錠可能な保管庫又は引き出し等への保管の対策を行うこと。

ウ 定期的に授業・研修用端末の存在確認を管理簿（様式１）を用いて行い、また持ち出す際及び返却する際は、管理簿（様式２）に記入すること。

（５） SUN ネット端末の管理

児童生徒が利用する SUN ネット端末の管理に関する具体的なセキュリティ対策については、別途定義する SUN ネットにおける小・中学校の iPad に関する実施手順に基づいて実施すること。

（６） その他のパソコン（図書端末、引落口座管理端末、チャイム管理端末、モバイル端末、外部電磁的記録媒体等）の管理

盗難防止のため、ワイヤーによる固定や施錠可能な保管庫又は引き出し等への保管の対策をおこなわなければならない。

（７） その他

ア 生体認証（顔認証）用の外付け Web カメラ等周辺機器は、紛失等がないように管理しなければならない。

イ 電磁的記録媒体については、情報が不必要になった時は、速やかに記録した情報を消去しなけれ

ばならない。

6 人的セキュリティ

(1) 教職員等の遵守事項

ア 教育情報セキュリティポリシー等の遵守

教職員等は、教育情報セキュリティポリシー及び実施手順等を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに教育情報セキュリティ管理者（学校・園、室課の長）に相談し、指示を仰がなければならない。

イ 業務以外の目的での使用の禁止

教職員等は、業務以外の目的で情報システムへのアクセス、電子メールの使用及びインターネットへのアクセスを行ってはならない。

ウ 端末等情報通信機器や電磁的記録媒体等の持ち出し、持ち込み、及び外部における情報処理作業の制限

(ア) 外部への持ち出しについて

a 校務用端末

学校外への持ち出しは原則禁止するものとし、持ち出す場合は教育情報セキュリティ管理者（学校・園、室課の長）の指示に基づいて行い、更に教育情報システム責任者（教育センター所長）に報告と了承を得た上で行うこと。

なお、持ち出しに際して、端末の紛失や盗難、第三者による画面ののぞき見等の情報漏洩の危険性について十分に理解したうえで細心の注意を払い、校務用端末の外部への持ち出しと利用を行うこと。

b 校務用端末（共用）

校務用端末（共用）を外部に持ち出すことを禁止する。

c 事務なび端末

所管部門（情報政策室）の指示に従い、外部への持ち出しを禁止する。

d 授業・研修用端末

授業・研修用端末を外部に持ち出すことは原則として禁止する。但し、校外学習などの学校行事や校外での教職員研修・研究発表等の場合、また教材研究や教材作成を校外で行うことが合理的と判断される等の場合は、以下の手順に従って、持ち出しを行うことができるものとする。

(a) 管理簿（様式2）に必要事項を記入し、教育情報セキュリティ管理者（学校・園、室課の長）の許可を得る。

(b) 校外において作成したデータは、端末等を学校に持ち帰り、データをサーバに保存した後、速やかに削除する。

(c) 授業・研修用端末を外部に持ち出した際、家庭や信頼できる場所以外の公衆通信回線（公衆無線LANやFreeWiFi等）に接続してはならない。

e その他情報通信機器、電磁的記録媒体

学校の端末、電磁的記録媒体、及び学校で購入したソフトウェア等を外部に持ち出すことは原則として禁止する。但し、校外学習などの学校行事や校外での研究発表等の場合は、以下の手順に従って、持ち出しを行う。

(a) 管理簿（様式3）に必要事項を記入し、管理職の許可を得る。

(b) 校外において作成したデータは、端末等を学校に持ち帰り、データをサーバに保

存した後、速やかに削除する。

(イ) 外部から校内への持ち込みについて

a 支給以外のパソコン、モバイル端末及び電磁的記録媒体

支給以外のパソコン、モバイル端末及び電磁的記録媒体等を業務に利用するために校内に持ち込むことを原則として禁止する。

但し、以下に例示する目的において、教育情報セキュリティ管理者（学校・園、室課の長）の許可を得て利用することができるものとするが、これらの機器を用いて作成した情報資産は、情報資産使用後に速やかに削除すること。

(a) 行事などで児童・生徒等を撮影するためのデジタルカメラ及びデジタルビデオの利用

(b) 行事などで児童・生徒の活動の様子等をブログシステムやホームページに更新するための携帯電話及びスマートフォン並びにタブレットの利用（重要性分類Ⅳの情報に限る）

(ウ) 外部における情報処理作業の制限について

a 自宅での情報資産持ち帰り処理

自宅で情報資産の処理は行ってはならない。但し、やむ得ない事情がある場合は、以下の手順に従い、自宅での情報資産処理を行う。

(a) 自宅パソコンで情報資産処理を行う場合、あらかじめ教育情報セキュリティ管理者（学校・園、室課の長）に許可を求めなければならない。（申請書）

(b) 持ち出す情報資産は、教材等の個人情報が含まれない重要性分類Ⅳのデータに限る。

(c) 自宅に持ち出した情報資産の処理は、自宅のみに限る。

(d) 自宅のパソコンについては、ウイルス対策ソフトをインストールし、最新のウイルス定義にした後、ウイルスチェックを事前実施しなければならない。

(e) 教材等作成した情報資産が不要になった場合は、端末内から速やかに削除する。

エ 端末等情報通信機器におけるセキュリティ設定変更の禁止

教職員等は、端末等情報通信機器に導入されたソフトウェアに関するセキュリティ機能の設定を教育情報システム管理者（教育委員会の情報システム担当室課の長）の許可なく変更してはならない。

オ 机上の管理

教職員等は、以下の事項に留意し、机上の管理を行わなければならない。

(ア) 日頃から机の上やパソコンの画面上に重要な情報を出したまませず、鍵のかかる机等に保管する。

(イ) 席を離れるときには、パソコンをログオフまたは電源を落とすようにする。

(ウ) パソコンに、電磁的記録媒体を接続したまま、離席しない。

カ クラウドサービス、ソーシャルメディアサービス利用制限

(ア) 私的に契約したクラウドサービスや個人アカウントを業務利用してはならない。

(イ) ソーシャルメディアサービスを利用して、業務上知り得た情報を公開してはならない。

(ウ) 利用するソーシャルメディアサービスごとの責任者を定めなければならない。

キ 児童生徒への指導事項

(ア) 学習用途の利用限定

学習用端末及び学習系クラウドサービスは学習目的で利用すること。

- (イ) 利用者認証情報の秘匿管理
 - ID 及びパスワードは他の人に知られないようにすること。
 - (ウ) ウイルス対策ソフトウェアの管理
 - ウイルス対策ソフトウェアは常に最新の状態に保つこと。
 - (エ) 端末のソフトウェアに関するセキュリティ機能の設定変更禁止
 - 利用する端末のセキュリティ機能の設定を、許可なく変更してはならないこと。
 - (オ) 学習系情報は学習系クラウドに保管
 - 端末で生成した情報の保存先を学習系クラウドに指定できる機能がある場合には、この機能を利用して原則学習系クラウドに保管し、学習者用端末にローカル保存は必要最小限とすること。
 - (カ) 外部ソフトウェアの無断インストール禁止
 - 無断で外部ソフトウェアをインストールしないようにすること。
 - (キ) コミュニケーションツールの利用制限
 - 学校から許可されたコミュニケーションツール（SNS、チャット等）のみを利用すること。
 - (ク) ウイルス感染が疑われる場合の報告
 - 学習用端末が動かない、勝手に操作されている、いつもと異なる画面や警告が表示されるなどの症状がでた場合、すぐに担任教員に報告すること。
 - (ケ) 端末の安全な取扱い
 - 学習用端末は大事に取り扱い、盗難・紛失・破損等に注意すること。
 - (コ) 私物端末など許可されていない端末の利用禁止
 - 私物端末など許可されていない端末を学校に持ち込んで、学校のネットワークにつながらないこと。
 - (サ) 重要性分類Ⅱ以上の情報資産（児童生徒本人の情報に限る）の管理
 - 該当資産を端末にダウンロードした場合には、目的を達成し次第速やかに消去を行う等の対策を講じること。また、該当資産を閲覧する際には、離席時に端末ロックし、周囲に他の児童生徒がいる状態では閲覧しない等の対策を講じること。
- ク 退職時等の遵守事項
- 教職員等は、異動、退職等により本校を離れる場合に、業務上知り得た情報を含むデータを持ち出してはいけない。また、本校を離れた後も、業務上知り得た情報を漏らしてはならない。
- (2) 情報セキュリティに関する研修
 - 教職員等は、毎年度最低 1 回は情報セキュリティ研修を受講するように努めなければならない。
 - (3) 情報セキュリティインシデントの報告
 - 教職員等は、個人情報の漏洩、学校 PC のウイルス感染、端末や公用 USB メモリ紛失等の情報セキュリティインシデントを認知した場合または、保護者や住民等外部から報告を受けた場合、速やかに教育情報セキュリティ管理者（学校・園、室課の長）に報告しなければならない。また教育情報セキュリティ管理者（学校・園、室課の長）は速やかに教育情報システム責任者（教育センター所長）に報告しなければならない。
 - (4) ID 及びパスワード等の管理
 - ア ID の取扱い
 - (ア) 教職員等は、自己の管理する ID を、他人に利用させてはならない。
 - (イ) 教職員等は、複数の利用者が共通で利用できる ID（以下、「共通 ID」という。）を利用する場合は、共通 ID の利用許可者以外に利用させてはならない。

- イ パスワードの取扱い
 - (ア) パスワードは、自分で責任を持って管理し、他人に教えない。
 - (イ) パスワードは十分な長さとし、文字の組み合わせは想像しにくいものにする。
 - (ウ) パスワードは、定期的に変更し、古いパスワードは再利用しない。また、パスワードが流出したおそれがある場合には、教育情報セキュリティ管理者（学校・園、室課の長）に速やかに報告し、パスワードを速やかに変更しなければならない。
 - (エ) 仮のパスワードは、最初のログイン時点で変更しなければならない。
 - (オ) パソコン等の端末にパスワードを記憶させない。
 - (カ) 教職員等間でパスワードを共有してはならない。（共通 ID は除く）
 - (キ) パスワードは、連続して 5 回間違えた場合、ログイン ID がロックされ、使用できなくなる。教職員等がパスワードを忘れた場合には、コールセンターに連絡し、パスワードを初期化するなど対応を依頼すること。
- (5) 学校内外での支給端末の運用ルールを制定し、インシデント時の連絡先対応方法を各学校にて整理し、実施手順に反映しなければならない。

7 技術的セキュリティ

(1) コンピュータ及びネットワークの管理

ア 電子メールの利用制限

- (ア) 電子メールはネットワーク上に点在するコンピュータを経由して配信されるため、その経路のどこかで他人に覗き見される恐れがあり、見られて困るようなメールは送らないこと。
- (イ) 教職員等は、外部メール機能を使い情報資産を外部に送信する場合は、必ず同報機能を利用し同じメール内容と添付ファイルを教育情報セキュリティ管理者（学校・園、室課の長）にも送らなければならない。
- (ウ) 教職員等は、メールにて、情報資産を送信する場合、パスワード等は、十分信頼できる方法により、相手方へ伝える必要がある。なお、重要性分類Ⅱ以上のデータについては、校務系サーバでパスワードを設定した上で、学習系サーバにある送信用フォルダに保存し、パスワードを解除せず送信しなければならない。送信後、データを速やかに削除する。
- (エ) 電子メールの利用について、判断に迷う場合は、教育情報セキュリティ管理者（学校・園、室課の長）に相談し、判断を仰がなければならない。

イ クラウドストレージの利用制限

- (ア) クラウドストレージは、許可されたサービスのみを利用可能とする。
- (イ) 許可するクラウドストレージサービスは以下の通りとし、それ以外の類似のクラウドストレージサービスは不許可とする。
 - a 許可するクラウドストレージサービス：Microsoft 社 OneDrive
- (ウ) 利用を許可するクラウドストレージは、学習系システムの位置付けにて利用を行うものとする。

ウ 情報の保存制限

不特定の教職員が利用することが想定される校務系端末のローカルディスクに、情報の保存は行ってはならない。

エ 無許可ソフトウェアの導入等の禁止

教職員等は、情報通信機器に無断でソフトウェアを導入してはならない。

オ 機器構成変更の制限

教職員等は、情報通信機器に対し機器の改造、増設及び交換を行ってはならない。

カ 機器設定変更の制限

教職員等は、情報通信機器に対して行われている機器設定の変更を許可なく行ってはならない。

特に、無線LANやルーター等のネットワーク環境は共用環境であり影響が大きいため、許可のない変更が無いように注意すること。

キ 無許可でのネットワーク接続の禁止

教職員は、情報通信機器が設定されていないネットワークに許可なく接続してはならない。
なお、マウスやキーボード等の入力装置に限り、Bluetoothを介した機器接続を許可する。

ク OSバージョンアップやパッチ適用

情報通信機器のOSバージョンアップやセキュリティパッチ適用は、ヘルプデスク等からの指示や案内に基づき実施すること。

(2) 不正プログラム対策

ア 教職員等の遵守事項

教職員等は、利用するに導入されている不正プログラム対策に関し、次のとおり取り扱わなければならない。

- (ア) 端末に導入されている不正プログラム対策ソフトウェアの設定を変更してはならない。
- (イ) 外部からデータ又は許可されたソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行うこと。
- (ウ) 差出人が不明又は不自然な添付ファイルを受信した場合は速やかに、教育情報セキュリティ管理者（学校・園、室課の長）を通じて、教育情報システム責任者（教育センター所長）に報告し、その指示に従い処理しなければならない。
- (エ) 不正プログラム対策ソフトウェアによるフルチェックを定期的実施すること。
- (オ) 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行うこと。
- (カ) 教育情報システム責任者（教育センター所長）が提供するウイルス情報を、校務支援システム上の掲示板や回覧等で常に確認すること。
- (キ) コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、次の対応を行ったうえ、教育情報セキュリティ管理者（学校・園、室課の長）を通じて、教育情報システム責任者（教育センター所長）に報告し、その指示に従わなければならない。
 - a 有線でネットワークに接続されている端末の場合
LAN ケーブルの即時取外しを行わなければならない。
 - b 無線でネットワークに接続されている端末の場合
直ちに利用を中止し、パソコンの電源を落とす、又は、Wi-Fi の接続を切る等、通信が行われないようにしなければならない。

8 運用

(1) 教育情報セキュリティポリシーの遵守状況の報告義務

教職員等は、教育情報セキュリティポリシー及び実施手順等に対する違反行為を発見した場合、直ちに教育情報セキュリティ管理者（学校・園、室課の長）に報告しなければならない。

(2) 法令遵守

教職員等は、職務の遂行において使用する情報資産を保護するために、次の法令等のほか関係法令

等を遵守し、これに従わなければならない。

ア 地方公務員法（昭和 25 年法律第 261 号）

イ 教育公務員特例法（昭和 24 年 1 月 12 日法律第 1 号）

ウ 著作権法（昭和 45 年法律第 48 号）

エ 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

オ 個人情報の保護に関する法律（平成 15 年法律第 57 号）

カ 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）

キ 吹田市個人番号の利用等に関する条例（平成 27 年条例第 24 号）

9 SaaS 型パブリッククラウドサービスの利用

(1) ホームページやブログの利用について

ア ホームページやブログの利用における対策の実施

イ 教職員等は、ホームページやブログを利用する場合は、教育情報システム責任者（教育センター所長）の定めたルールに従い、利用しなければならない。

ウ 重要性分類Ⅰ又はⅡの情報は、ホームページやブログで発信してはならない。

(2) SaaS 型パブリッククラウドサービス利用における教職員等の留意点

ア ID 及びパスワード等の秘匿

(ア) 教職員等は、ID 及びパスワードについて秘匿管理を行わなければならない。

(イ) 教職員等は、多要素認証に必要な要素（知識、生体、物理）についても適切に管理を行わなければならない。なお、該当要素が流出等したと考えられる場合には、速やかに教育情報セキュリティ管理者に報告しなければならない。

イ モバイル端末の持ち歩きリスク

教職員等は、クラウドサービスにアクセスする際に使用するモバイル端末について、紛失・盗難を避けるよう、適切に管理しなければならない。

ウ 重要性分類に基づく情報管理

パブリッククラウド上で重要な情報(重要性分類Ⅱ以上)を取り扱う際には、多要素認証を含む強固なアクセス制御による対策を講じなければならない。ただし、児童生徒又はその保護者が重要性分類Ⅱ以上の情報資産にアクセスする場合は、児童生徒本人又はその保護者が、当該児童生徒に関するもののみにアクセスすることを想定していることから、多要素認証を設定することが望ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID 及びパスワードでの認証を許容する。

エ 学校外からのパブリッククラウド利用

(ア) 教職員等は、学校外からクラウドサービスを利用する際、情報資産の取扱いをクラウドサービス上のみで行うことを原則とする。

(イ) クラウドサービスから端末にファイルをダウンロードする際は、情報資産の外部持ち出しに基づく安全管理措置として、端末の安全性を事前に確認するとともに、作業が終わり次第当該端末から情報資産を速やかに消去しなければならない。

オ SaaS 型パブリッククラウドサービスの学習用途、校務用途混在リスクへの対応

(ア) 教職員等は、強固なアクセス制御による対策を講じたシステム構成にてクラウドサービスを利用している場合には、クラウドサービスを学習用途と校務用途で適切に使い分けるよう、

共有先やダウンロード方法等の運用ルールについてあらかじめ確認し、適切に運用しなければならない。

(イ) 教職員等は、ネットワーク分離による対策を講じたシステム構成で、クラウドサービスを利用している場合には、クラウドサービスを学習用途と校務用途で使い分けるよう、適切に運用しなければならない。

1 0 評価・見直し

教職員等は、教育情報セキュリティ管理者（学校・園、室課の長）から提示される自己チェックシートの活用等の自己点検を行い、その結果に基づき、自己の権限の範囲内情報セキュリティ対策について改善を図らなければならない。

1 1 参考資料

吹田市教育委員会の組織体制の図を以下に示す。

