吹田市立南山田学校教育情報セキュリティ対策実施手順書

令和７年４月１日作成

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、教職員等が順守すべき具体的な事項を定めるものである。

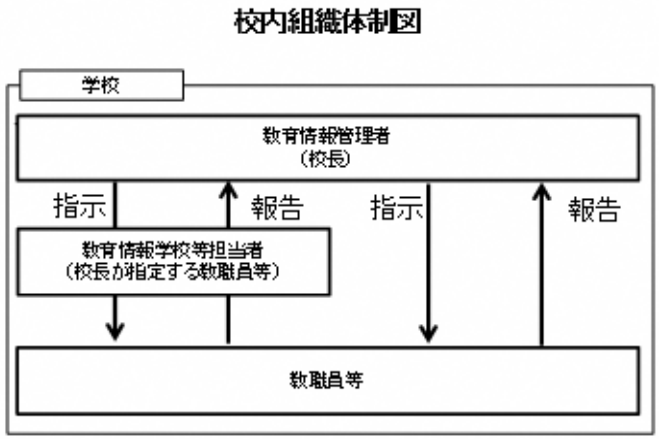
教職員等は、この実施手順を順守し、情報セキュリティを確保しなければならない。

２　定義

用語	定義
教育情報システム	校務系システム及び学習系システムを合わせた総称
校務系システム	校務系サーバ、校務系サーバと通信を行っているパソコン等の端末及びソフトウェアで構成される校務系情報を取り扱うシステム、通称SATSUKIネットシステムという
学習系システム	学習系サーバ、学習系サーバと通信を行っているパソコン等の端末及びソフトウェアで構成される学習系情報を取り扱うシステム、通称SUNネットシステムという
校務系サーバ	校務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
情報通信機器	情報処理・通信機能を持つパソコン等の端末やネットワーク機器及びそれらの周辺機器の総称
校務用端末	校務系サーバと通信を行っている教職員が利用するパソコン等端末
校務用端末（共有用）	校務系サーバと通信を行っている各学校に配備されている共有用パソコン等端末
事務なび端末	校務系サーバと通信を行うことが可能な市教委職員が利用するパソコン等端末 ただし、本端末の管理については情報政策室が所管する
授業・研修用端末	学習系サーバと通信を行っている教職員が利用するパソコン等端末
SUNネット端末	学習系サーバと通信を行っている児童生徒が利用するパソコン等端末
校務系情報	児童･生徒の成績、健康診断結果、指導要録、教職員等の個人情報など、学校が保有する電子データのうち、それら情報を学校・学級の管理運営、学習指導、生徒指導、生活指導、進路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
学習系情報	学校が保有する電子データのうち、保護者メール、出欠席及びその理由、学校ホームページ等インターネット接続を前提とした情報、及び児童・生徒のワークシート、作品など、学校が保有する電子データのうち、学校における授業など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等及び児童・生徒がアクセスすることが想定されている情報
電磁的記録媒体	DVD、公用USBメモリ、デジタルカメラ、デジタルビデオ等の記録媒体

３　校内組織体制

校内の組織体制の図を以下に示す。



４　電子データ（※当該電子データの印刷物も含む）の分類及び管理

(1)　電子データの分類

電子データを重要性に応じ次のとおりに分類する。個人情報を含むデータは、校務系サーバで取り扱う。

但し、学校の業務上の特性から、万が一の流出の際に影響が軽微な個人情報を含む重要性区分Ⅲの情報については、運用上の決まりを守り、学習系サーバでも取り扱えることとする。

重要性区分	内容	保存場所	該当する電子データの例示	備考
Ⅰ	セキュリティ侵害が、教職員等又は児童･生徒の生命、財産、プライバシー等へ重大な影響を及ぼす電子データ	校務系サーバ	・指導要録原本 ・教職員等の人事情報	
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電子データ	校務系サーバ	○学籍関係 ・出席簿 ・卒業証書授与台帳 ・転退学受付（整理）簿 ・転入学受付（整理）簿 ・就学児童・生徒異動報告書 ・教科用図書給付児童･生徒名簿	

			・要・準要保護児童・生徒認定台帳 ・その他校内就学援助関係書類 ○成績関係 ・評定一覧表 ・定期考査素点表 ・成績に関する個票等 ・通知表 ・定期考査・テスト等の問題及び用紙 ○指導関係 ・事故報告書・記録簿 ・生徒指導・特別指導等記録簿 ・児童・生徒等の個人写真・集合写真 ・指導記録等 ・教育相談・面接の記録等 ・個別の教育支援計画 ・個別指導計画 ・家庭訪問記録・個別面談記録 ・教務手帳 ・週ごとの指導計画 ○進路関係 ・卒業生進路先一覧等 ・進路希望調査 ・進路判定会議資料 ・進路指導記録簿 ・調査書 ・推薦書 ・私立高校入試に係る事前相談資料 ・入学者選抜に関する表簿（願書等） ○健康関係	・個人情報が含まれるもの

			・健康診断に関する表簿 ・健康診断票 ・歯の検査表 ・心臓管理等医療情報 ・学校生活管理指導票 ・児童・生徒等健康調査票 ・児童・生徒の健康保険等被保険者証の写 ○児童・生徒に関する個人情報 ○学校教職員等に関する個人情報 ○名簿等 ・生徒・児童名簿 ・生徒・児童の住所録 ・座席表 ・PTA 会員名簿 ・職員緊急連絡網・職員住所録 ・委員会・クラブ名簿 ○児童・生徒の学習系情報 ・学習活動の記録 ・学校行事等の児童・生徒の写真 ○その他 ・給食関係書類 ・学校徴収金会計簿	・生活歴、心身の状況、財産状況等の情報、電話番号、ﾒｰﾙｱﾄﾞﾚｽ、住所、氏名、生年月日、性別等 ・住所、電話番号、性別等 ・評価に使用するもの
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電子データ	学習系 サーバ（一時的に端末内も含む） もしくは 校務系 サーバ ※事務職員と共有する電子	○学籍関係 ・出欠及びその事由 ○児童・生徒の学習系情報 ・児童・生徒の学習記録（ワークシート、レポート、作品等） ・学習活動の記録 ○学校運営関係	・児童生徒が作成中のもの ・写真等の個人情報を含むもの

		データは校務系サーバに保存する必要がある。	・特色紹介冊子原稿 ・PTA資料 ・学園・学校・学年・学級だより ・卒業アルバム ・学校行事等の児童・生徒の写真 ・学校運営に関するアンケート ・教育委員会が指定するオンライン会議システムで撮影した運動会等の動画・写真 ・授業用教材 ・学校行事のしおり ・教材研究資料	・写真等の個人情報を含むもの ・写真等の個人情報を含むもの ・保護者・地域説明や児童に前年の活動の様子を伝えるために使用する場合に限る ・写真等の個人情報を含むもの ・宿泊学習のしおり、式次第 ・写真等の個人情報を含むもの
Ⅳ	上記以外の電子データ	学習系 サーバ（一時的に端末内も含む） もしくは 校務系 サーバ ※事務職員と共有する電子データは校務系サーバに保存する必要がある。	○学校運営関係 ・学校要覧 ・学校紹介パンフレット ・使用教科書一覧 ・教育課程編成表 ・学校行事実施計画 ・保護者等への配布文書文例 ・各種届出用紙雛形 ・校務分掌表 ・学校・学園ホームページ掲載情報 ・学校行事のしおり ・授業用教材 ・教材研究資料 ・児童・生徒用配布プリント ・週ごとの指導計画	・個人情報は含まないもの

(2)　電子データの管理方法

ア　電子データの管理(取扱い)

教職員等は、保管している電子データについて、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、電子データを複製した場合には、複製した電子データも、同様に取り扱わなければならない。

電子データの分類		電子データの管理（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
重要性区分	定義	禁止	制限	電子メールでの送信	電磁的記録媒体の運搬	自宅パソコンでの電子データ処理					
Ⅰ	セキュリティ侵害が教職員等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管理者（校長等）の許可で持ち出しを可	暗号化、パスワード設定を行う	禁止	禁止	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、耐湿を講じた施錠可能な場所に保管 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	電磁的記録媒体の物理的な破壊、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。	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軽微な影響を及ぼす。	特になし	同上 但し、やむを得ない場合、教育情報管理者（校長等）の許可で可	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	影響をほとんど及ぼさない。	同上	教育情報管理者（校長等）の確認のもと可	特になし	教育情報管理者（校長等）の許可で可	教育情報管理者（校長等）の許可で可	特になし	同上	同上	特になし	特になし

イ　電子データの作成

（ア）　教職員等は、業務上必要のない電子データ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、教育情報管理者（校長等）に許可を得たこと。

（ィ）　電子データを新規作成する教職員等は、（２）アの表に基づき、取り扱わなければならない。

（ゥ）　電子データを新規作成する教職員等は、作成途上の電子データについても、紛失や流出等をさせてはならない。また、電子データの作成途上で不要になった場合は、当該電子データを消去しなければならない。

ウ　電子データの入手

（ァ）　教職員等は、自校の教職員等から電子データを入手した場合は、重要性区分に基づいた取扱いをしなければならない。

（ィ）　学校外の者が作成した電子データを入手した教職員等は、（２）アの表に基づき、当該電子データを取り扱わなければならない。

（ゥ）　電子データを入手した教職員等は、入手した電子データの重要性区分が不明な場合、教育情報管理者（校長等）に判断を仰がなければならない。

エ　電子データの利用

（ァ）　電子データを利用する教職員等は、業務以外の目的に電子データを利用してはならない。

（ィ）　電子データを利用する教職員等は、電子データの重要性区分に応じ、取扱いをしなければならない。

（ゥ）　電子データを利用する教職員等は、電磁的記録媒体に電子データの重要性区分が異なる電子データが複数記録されている場合、記録されている電子データのうち重要性区分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。

オ　電磁的記録媒体の保管

（ァ）　教職員等は、電子データの重要性区分に従って、電子データを保管しなければならない。

（ィ）　教職員等は、電子データを記録した電磁的記録媒体を長期保管する場合は、電子データが改ざんされないように保管しなければならない。

（ゥ）　教職員等は、重要性区分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。

カ　電子メールでの送信

重要性区分Ⅰ、Ⅱ又はⅢの情報を外部へ送信する場合は、教育情報管理者（校長等）の許可を得たうえで、暗号化又はパスワード設定を行わなければならない。

キ　電磁的記録媒体の運搬

（ァ）　重要性区分Ⅰ又はⅡの電子データの学校外への運搬は、禁止する。

（ィ）　重要性区分Ⅲ又はⅣの電子データ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、電子データ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。

（ゥ）　重要性区分Ⅲ又はⅣの電子データ（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、教育情報管理者（校長等）の許可を得なければならない。

ク　電子データの提供・公表

（ァ）　重要性区分Ⅰの電子データは、外部に提供できない。

（ィ）　重要性区分Ⅱ又はⅢの電子データ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。

（ゥ）　重要性区分Ⅱ又はⅢの電子データを外部に提供する時は、教育情報管理者（校長等）に許可を得なければならない。

（ェ）　保護者や地域に公開する電子データについて、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。

ケ　電磁的記録媒体の廃棄

（ァ）　重要性区分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、電子データ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。

（ィ）　重要性区分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。

（ゥ）　重要性区分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、教育情報管理者（校長等）の許可を得なければならない。

(3)　電子データ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区分Ⅲの電子データ）

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電子データについて、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。

（ァ）　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こと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。

（ィ）　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。

（ゥ）　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電子データについて、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。

(4)　電子データ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、教育情報管理者（校長等）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　物理的なセキュリティ対策

(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、別途定義する以下の実施手順に基づいて実施すること。

ア　SUN ネットにおける小学校の iPad に関する実施手順※小学校の場合

イ　SUN ネットにおける中学校の iPad ・WindowsPC に関する実施手順※中学校の場合

(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　人的なセキュリティ対策

(1)　教職員等の順守事項

ア　教育情報セキュリティポリシー等の順守

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順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、順守することが困難な点等がある場合は、速やかに教育情報管理者（校長等）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管理者（校長等）の指示に基づいて行い、更に教育センター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)　記録簿（様式４）に必要事項を記入し、教育情報管理者（校長等）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)　記録簿（様式４）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。

（ィ）　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、教育情報管理者（校長等）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電子データは、電子データ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）

（ゥ）　外部における情報処理作業の制限について

a　自宅での電子データ持ち帰り処理

自宅で電子データ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、自宅での電子データ処理を行う。

(a)　自宅パソコンで電子データ処理を行う場合、あらかじめ教育情報管理者（校長等）に許可を求めなければならない。（申請書）

(b)　持ち出す電子データは、教材等の個人情報が含まれない重要性区分Ⅳのデータに限る。

(c)　自宅に持ち出した電子データの処理は、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に実施しなければならない。

(e)　教材等作成した電子データ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（情報システム担当室課の室課長）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。

（ァ）　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にせず、鍵のかかる机等に保管する。

（ィ）　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。

（ゥ）　パソコンに、電磁的記録媒体を接続したままで、離席しない。

カ　退職時等の順守事項

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、速やかに教育情報管理者（校長等）を通じて、統括教育情報セキュリティ責任者（学校教育室長）に報告しなければならない。また、必要に応じて教育情報管理者（校長等）を通じて、教育情報システム管理者（各室課長）にも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

（ァ）　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。

（ィ）　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

教職員等は、自己の管理するパスワードに関し、次の事項を順守しなければならない。

（ァ）　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。

（ィ）　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。

（ゥ）　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、教育情報管理者（校長等）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。

（ェ）　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。

（ォ）　パソコン等の端末にパスワードを記憶させない。

（ヵ）　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。

7　技術的なセキュリティ対策

(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電子データ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管理者（校長等）にも送らなければならない。

（ウ）　教職員等は、メールにて、電子データを送信する場合、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、重要性区分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。

（オ）　電子メールの利用について、判断に迷う場合は、教育情報管理者（校長等）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　教職員等の順守事項

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、教育情報管理者（校長等）を通じて、統括教育情報システム管理者（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に実施すること。

（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）　統括教育情報システム管理者（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、教育情報管理者（校長等）を通じて、統括教育情報システム管理者（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　運用面におけるセキュリティ対策

(1)　教育情報セキュリティポリシーの順守状況の報告義務

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、直ちに教育情報管理者（校長等）に報告しなければならない。

(2)　法令順守

教職員等は、職務の遂行において使用する電子データを保護するために、次の法令等のほか関係法令等を順守し、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　吹田市個人情報保護条例（平成 14 年条例第 7 号）

ク　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　外部サービスの利用

ホームページやブログの利用について

(1)　ホームページやブログの利用における対策の実施

教職員等は、ホームページやブログを利用する場合は、統括情報システム管理者（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。

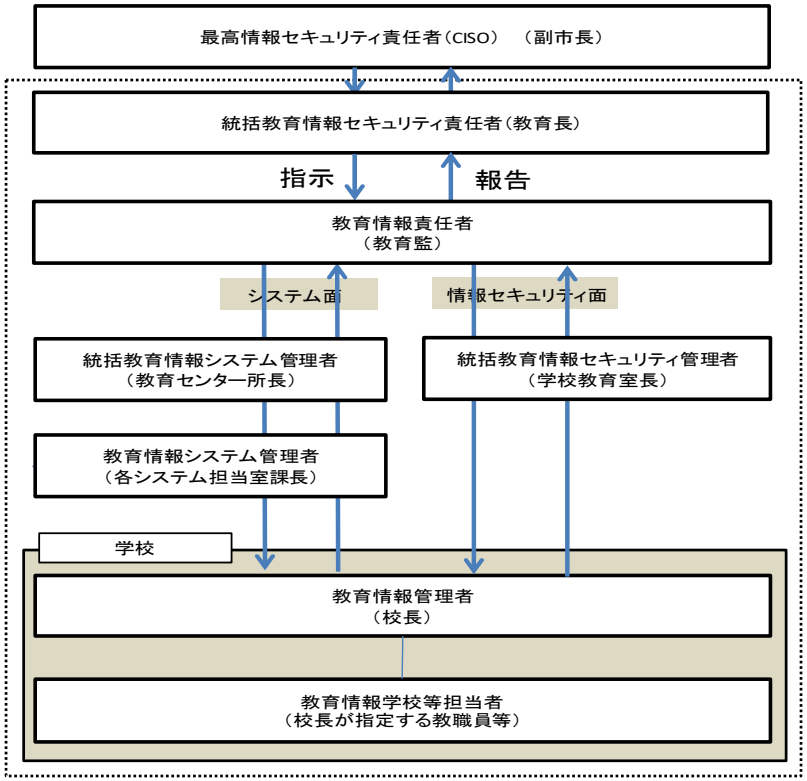
(2)　ホームページやブログを利用した情報の発信について

重要性区分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。

１０　自己点検及び結果の活用

教職員等は、教育情報管理者（校長等）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。

１１　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。

組織体制図