枚方市立樟葉小学校
情報セキュリティ対策実施手順書

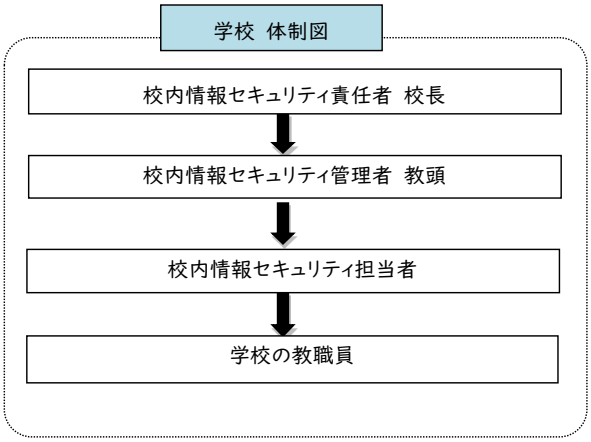
改 訂 履 歴			
初版	平成25年10月1日	改訂 6	令和 3年 4月 1日
改訂 1	平成27年4月 1日	改訂 7	令和 4年 4月 1日
改訂 2	平成27年 6月18日	改訂 8	令和 6年 4月 1日
改訂 3	平成31年 4月 1日	改訂 9	令和 7年 4月 1日
改訂 4	令和 1年10月 1日		
改訂 5	令和 2年 7月14日		

目次

書式を変更: フォント : 太字（なし）

Ⅰ.情報セキュリティ対策実施手順書の位置付けと学校の体制図について

文書名		内容
枚方市立学校情報セキュリティポリシー	情報セキュリティ基本方針	学校のセキュリティ対策の目的や原則を定めた統一的な規範
	情報セキュリティ対策基準	学校にある情報を脅威から守るための具体的な対策を示したもの
枚方市立学校情報セキュリティ対策基準等 運用マニュアル		情報セキュリティ対策基準を適正かつ円滑に管理・運用するために各項に対する解説を示したもの
各学校の情報セキュリティ対策実施手順書		学校において情報セキュリティ対策を実行するために各教職員が行動する手順を示したもの



実施手順

- **校内情報セキュリティ責任者（校長）は、学校の情報セキュリティ実施手順書を策定する。**
- **校内情報セキュリティ責任者（校長）は、所属の教職員から校内情報セキュリティ担当者を 1 名選任して、教育研修課に報告する。**
- **校内情報セキュリティ管理者（教頭）は、校内情報セキュリティ責任者（校長）を補佐して、所属する教職員の情報セキュリティ対策の実施について管理、指導を行う。**
- **校内情報セキュリティ担当者は、校内情報セキュリティ責任者（校長）及び校内情報セキュリティ管理者（教頭）と協力して、学校情報セキュリティポリシーの順守遵守及び周知・啓発に努め**

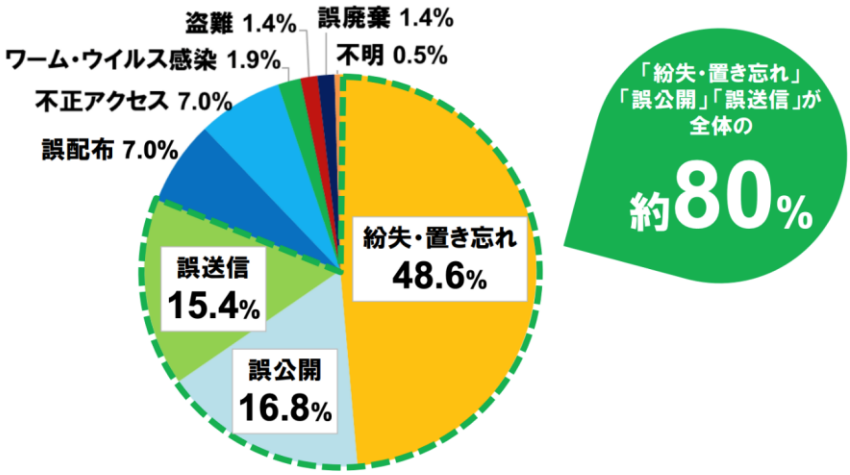
2. 校内情報セキュリティ研修の実施について

情報セキュリティに関する事故の多くが、教職員等の故意又は過失による規程違反に起因している現状から、情報セキュリティを適切に確保するためには、情報セキュリティ対策の必要性と対策の内容を教職員等（学校事務職員や非常勤講師、NET等も含め）が十分に理解していることが必要です。

情報セキュリティの向上は、利便性の向上とは、必ずしも相容れない場合が多く、業務効率を優先すると情報セキュリティ対策の軽視につながることもあります。

情報セキュリティに関する脅威や技術の変化は早く、教職員等は常に最新の状況を理解しておくことが求められます。そのことから、校内情報セキュリティ責任者（校長）は、必ず校内情報セキュリティ研修や実際に事故が発生した場合に的確に対応できるようにするため、緊急時に対応した訓練を実施する必要があります。

個人情報漏えいの原因



（出典 教育ネットワーク情報セキュリティ推進委員会.令和5年度（2023年度）学校・教育機関における個人情報漏えい事故の発生状況－調査報告書－第1.1版.2024年7月24日. https://school-security.jp/wp/wp-content/uploads/2024/06/2024_1.pdf.2025.2.11参照 ~~ISEN2023 年 学校における個人情報漏えい事故の発生状況 －調査報告書より~~）

実施手順

- **校内情報セキュリティ責任者（校長）は、学校で校内情報セキュリティ研修を必ず実施する。**
- **個人情報の漏えいの多くが、人為的ミスであることを理解しておきましょう。**
- **すべての教職員等（事務職員や非常勤講師、NET等も含め）は情報セキュリティに関する校内研修を必ず受講しましょう。**
- **校内情報セキュリティ研修を実施した日時、受講者の記録をしましょう。**

書式を変更: フォント : 8 pt
書式を変更: フォント : （英）UD デジタル 教科書体 NK-R, （日）UD デジタル 教科書体 NK-R, 8 pt
書式を変更: フォント : 8 pt
書式を変更: フォント : （英）UD デジタル 教科書体 NK-R, （日）UD デジタル 教科書体 NK-R, 8 pt
書式を変更: フォント : 8 pt
書式を変更: フォント : （英）UD デジタル 教科書体 NK-R, （日）UD デジタル 教科書体 NK-R, 8 pt
書式変更: 右揃え, インデント : 最初の行 : 1 字
書式を変更: フォント : 8 pt
書式を変更: フォント : （英）UD デジタル 教科書体 NK-R, （日）UD デジタル 教科書体 NK-R, 8 pt
書式を変更: フォント : 8 pt
書式を変更: フォント : （英）UD デジタル 教科書体 NK-R, （日）UD デジタル 教科書体 NK-R, 8 pt
書式を変更: フォント : 8 pt
書式を変更: フォント : 8 pt
書式を変更: フォント : 8 pt
書式を変更: フォント : 8 pt

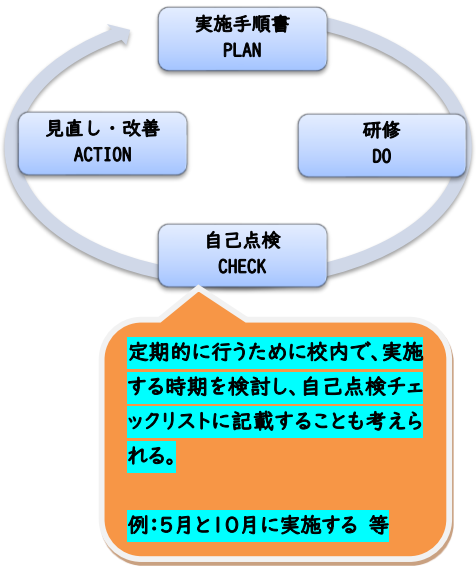
3. 自己点検の実施について

枚方市立学校情報セキュリティポリシーの履行状況等を自ら点検、評価することは、枚方市立学校情報セキュリティポリシーの~~順守~~遵守事項を改めて認識できる有効な手段です。自己点検は、情報システム等を運用する者又は利用する者自らが実施するもので、監査のような客観性は担保されませんが、監査と同様に、点検結果を踏まえ各部門で改善を図ったり、学校全体のセキュリティ対策の改善を図る上での重要な情報になる情報セキュリティ対策の評価を行い、対策の見直しに資するものです。また、教職員等の情報セキュリティに関する意識の向上や知識の習得にも有効です。

自己点検は、校内情報セキュリティ責任者が所属する学校の教職員を対象に、定期的かつ必要に応じて実施します。

自己点検・内部監査のフロー

情報セキュリティ実施手順書の策定・改正
⇩
情報セキュリティ研修
⇩
実施手順書に基づく
自己点検チェックリストの作成
⇩
自己点検の実施　各校長・教職員
⇩
情報セキュリティ内部監査
⇩
実施手順書の見直し・改善



実施手順

- **校内情報セキュリティ責任者（校長）は、所属する教職員等（学校事務職員や非常勤講師等を含め）に対して定期的に自己点検を実施する。**
- **教職員等は自己点検チェックリストに基づいて、情報セキュリティ実施手順書どおりに運用できているか確認しましょう。**

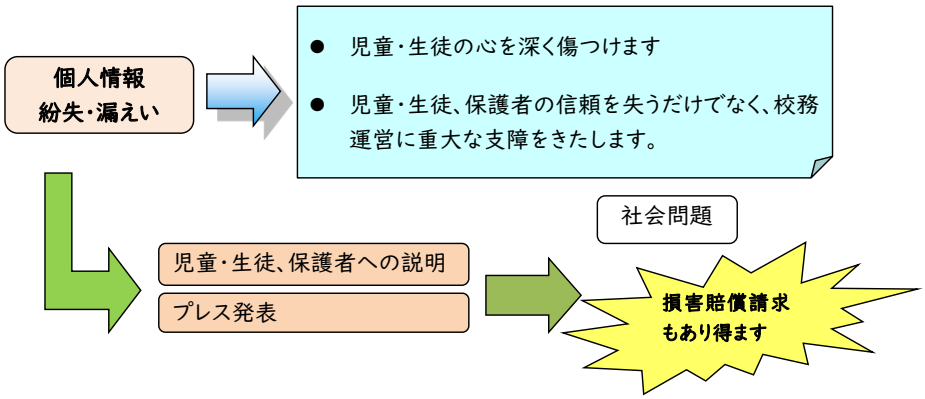
4. 電子データの個人情報漏えい防止について

日常的に多くの学校情報や成績等を取り扱う教職員は、教育公務員として幅広い見識と高い実践力が求められています。個人情報の紛失はもちろんのことですが、カバン等の盗難事故にあった場合でもそのカバンの中に児童・生徒の個人情報の入った端末やUSBメモリなどが入っていれば、児童・生徒に対する加害者となってしまいます。

万が一、個人情報が流出した場合、児童・生徒本人だけでなくその家族にまで被害が及ぶおそれがあります。

一人ひとりの教職員が個人情報の適正な取扱について常に心がけておくことが大切です。

個人情報が漏えいした場合



個人情報が紛失・漏えいしてからでは、取り返しがつきません。

実施手順

- **児童・生徒等の個人情報は、枚方市立学校情報セキュリティポリシーに基づいて適切に取り扱いましょう。~~を持ち出さないようにしましょう。~~**
- **個人情報の扱い方について、日頃から校内で共通理解をもっておきましょう。**
- **使用頻度の少ないものは、DVD等のメディアに保存し、施錠可能な場所に保管しましょう。**

5. 記録媒体の使用の制限について

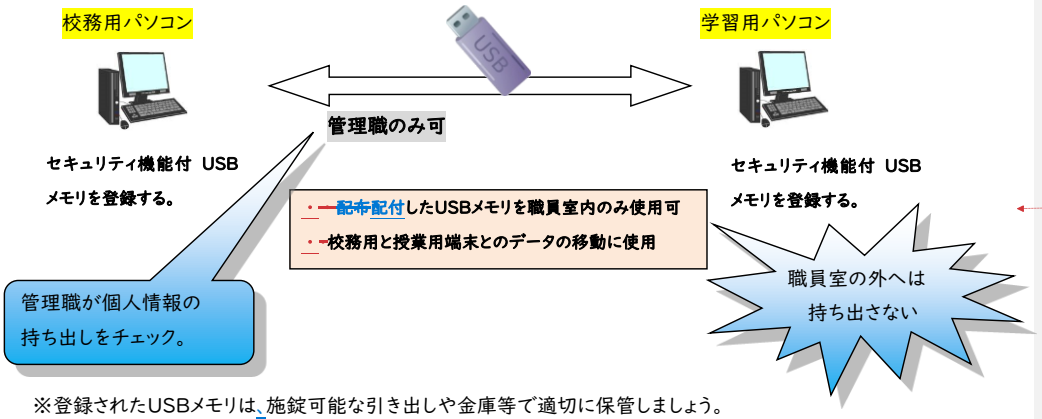
USBメモリについては、教育委員会から配備されたUSBメモリとオルガン用やプログラムタイマー用のUSBメモリのみが使用可能です（下図参照）。

私物USBメモリ・私物コンピュータの学校内への持込は禁止されています。

自宅で作成した教材や書類（※個人情報を含まないもの）に関しては、学校のメールアドレスや教職員へ貸与しているメールアドレスへ送る方法等~~やCD－R、DVD－R等に保存して持ってくる方法~~があります。

逆に、校務用端末から学校の教材や書類（※個人情報を含まないもの）を自宅メールアドレスや教職員へ貸与しているメールアドレスへ送る場合は、管理職の承認が必要となります。

教育委員会配備USBメモリ



※登録されたUSBメモリは、施錠可能な引き出しや金庫等で適切に保管しましょう。

USB端子を利用するデジタルカメラやICレコーダー、フロッピーディスクドライブ等の周辺機器は登録されたものしか使用することはできません。

また、デジタルカメラ等で使用するSDカードについては、端末機からデータを外部に持ち出すことを防ぐため、読み取り専用になっています。読み取りできない場合は、管理職を通じて教育研修課へ登録の依頼が必要です。

教育内部系~~（校務用）の~~端末（校務用端末）内蔵のDVDドライブについても読み取り専用となっています。

実施手順

- **私物USBメモリや私物PCのを学校への持込みは禁止されています。~~まないようにしましょう。~~**
- **学習用PC⇔校務用PC間のデータ移動には、教育委員会配備USBメモリを使いましょう（校務用PCのDVDドライブは読み取り可能です）。**
- **教育委員会配備USBメモリは職員室の外へは持ち出さないようにしましょう。保管等は、施錠可能な引き出しや金庫等で保管しましょう。**

書式変更：インデント：左：0 mm，最初の行：0字

6. ウイルス対策について

ウイルス対策については、感染の監視やウイルス除去等の作業を学校㊢ヘルプデスクに委託しており、ウイルスを感知した場合、委託業者から連絡があります。

市立~~内~~小中学校のコンピュータにはウイルス対策ソフト（ウイルスバスター）が入っており（OSの特性により、対策を行う）、コンピュータ起動時にプログラムは自動更新されるようになっています。長い間コンピュータを使用していない場合は、この更新にさらに時間がかかります。

その更新中に、別の操作をしていて、ウイルスに感染する場合があります。使用しなくても、少なくとも1週間に一度はコンピュータを起動させることが必要です。

具体的な感染例

- インターネットに接続した（Webサイトを閲覧した）だけでウイルスに感染する。
- ウイルスに感染したコンピュータが接続されているとネットワーク全体に感染が広がり、他のコンピュータもウイルスに感染する。
- メールの添付ファイルを開くだけで、ウイルスに感染する。
- USBメモリにウイルスが入っている場合、差し込んだだけで感染する。

学校のウイルス対策に関する委託業者
学校㊢ヘルプデスク　内線15−8092（IP電話から）
050−7105−8092

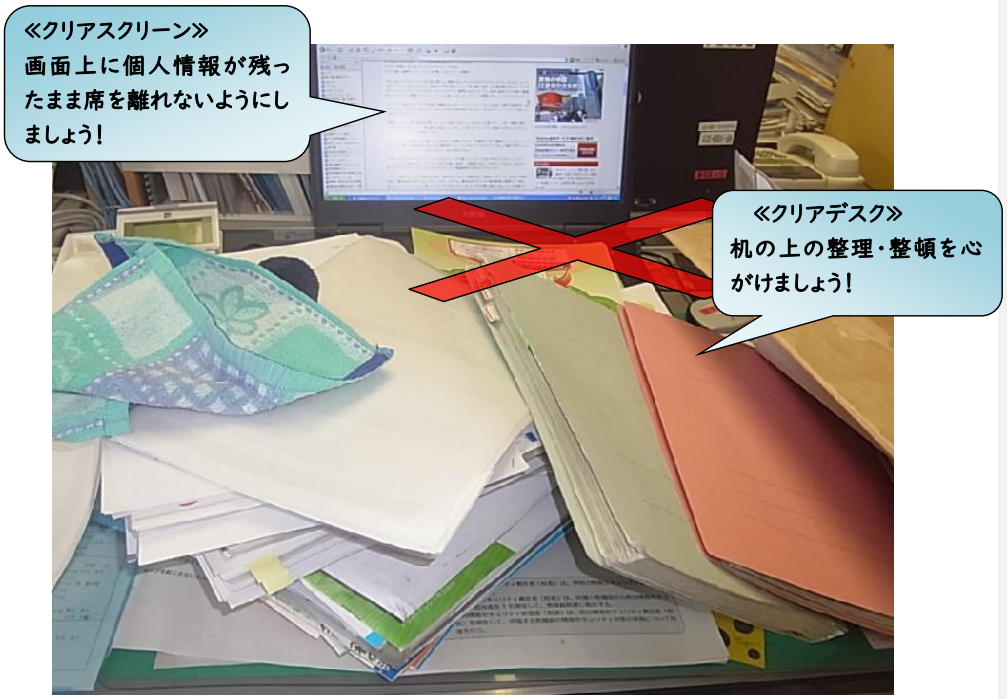
実施手順

- **私物のUSBメモリの学校~~内~~への持ち込みは禁止されています。**
- **仕事に関係ないホームページのサイトは見ないようにしましょう。**
- **知らない相手からのメールの添付ファイルは、注意しましょう。**
- **自動更新のため少なくとも１週間に一度は、起動させるようにしましょう。**
- **自宅で文書を作成する場合には、自宅コンピュータにもウイルス対策をしましょう。**

7.クリアデスク及びクリアスクリーンの実施について

出入りの多い職員室の机の上などに個人情報が記載された文書・電子媒体などを放置しないこと（クリアデスク）や、コンピュータの画面上に重要な情報が表示されたままにしないこと（クリアスクリーン）を職員全員で実施することが、情報セキュリティの強化につながります。

クリアデスクについては、一時的な対応で終わってしまう恐れがあるので、日頃から習慣づけて行っていくことが必要です。また、クリアスクリーンについては、スクリーンセイバーを使用することが便利です。長時間、離席する際には、電源のオフはもちろんログオフやノート型コンピュータの蓋をしめておくこと、教育内部系~~（校務用）~~端末（校務用端末）については、ICカードを抜いておくことが考えられます。



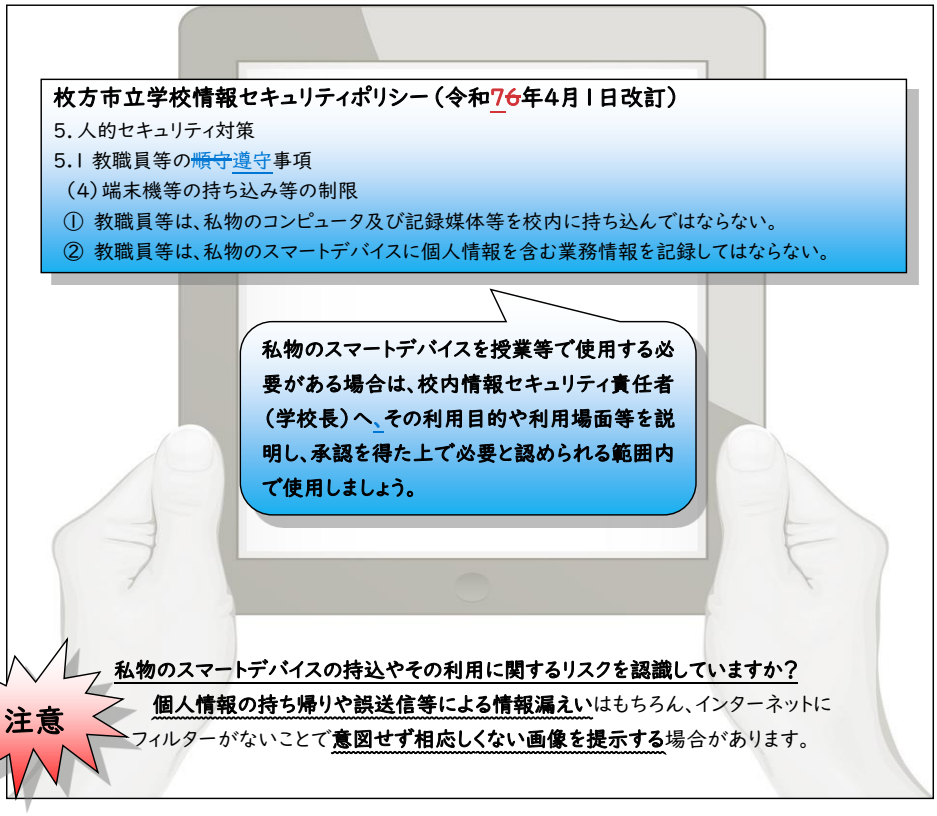
実施手順

- **日頃から机の上や、コンピュータの画面上に重要な情報を出したままにしないように、管理、整理をしましょう。**
- **長時間、席を離れる時にはシャットダウンまたはICカードを抜いておきましょう。**
- **書類を処分するときには、一つひとつチェックして個人情報が入っていないか確認しましょう。**

8. 私物スマートデバイス（スマートフォンやタブレット等）について

~~情報通信技術の進展に対応するため令和3年4月1日付で情報セキュリティポリシーが改訂されました。その内容は近年急速に普及しているスマートデバイス（スマートフォン及びタブレット型コンピュータ）についても通常のコンピュータと異なる環境での使用が想定されるため、学校においての利用条件やセキュリティ対策が追加されました。~~

~~あわせて、~~教職員等の私物スマートデバイスも使用方法によっては、情報漏えい等の事故につながる危険性が~~あるため、~~あります。そのため、枚方市立学校情報セキュリティポリシーでは、人的セキュリティ対策として、教職員等の私物端末等の持ち込みや業務中の使用における禁止事項を明記しています。~~業務中の利用における禁止事項が明記されています。~~



実施手順

- **私物スマートデバイスに個人情報を含む業務情報を記録してはいけません。**
- **私物のスマートデバイスで校内ネットワーク及びコンピュータへの接続（充電目的の接続を含む）をしてはいけません。**

9. USB メモリ等外部記録媒体の適正管理について

校内情報セキュリティ責任者は、USB メモリ等外部記録媒体に個人情報を記録し、外部に持ち出したりする場合~~に個人情報を記録する際~~には、「様式第 3 号 外部記録媒体利用申請書」を学校情報セキュリティ管理者に提出しなければいけません。また、学校図書館システムへ氏名等の利用者情報をデータ転送する際には申請が必要です。

学校用 USB メモリ、外付けハードディスク等の外部記録媒体は、施錠可能な保管庫に保管するなどの盗難防止対策をとらなければいけません。適切に管理・使用するために管理台帳と使用簿の作成が必要です。

対象となる記録媒体には、管理番号を記したラベルを貼って管理する必要があります。※管理台帳等は、グループウエアのファイル管理内のものをひな型として作成しています~~する~~。

外部記録媒体管理台帳（外部記録媒体一覧）

学校名

記入例

管理番号	○○小（学校名）−HDD（種別）1（番号） ※種別例 DVD、USB	記録媒体の種類	外付けハードディスク
ファイル名称	○○○.jpg他 ○件	記録内容	画像等
利用目的	ホームページ用	保管場所	校長室金庫
保管期間	（使用開始日）R○年○月○日～（廃棄日）R○年○月○日		

外部記録媒体使用簿

学校名

NO	使用年月日	返却日	管理番号	使用者	使用用途	確認者
例	R○年○月○日	R○年○月○日	○○小（学校名） DVD（種別）2(番号)	○○○	学校便り作成	○○○
1	R 年 月 日	R 年 月 日				
2	R 年 月 日	R 年 月 日				

実施手順

- **USB メモリ等に個人情報を記録し、外部に持ち出したりする場合は、「様式第 3 号 外部記録媒体利用申請書」を提出しましょう。**
- **個人情報を記録・保存するための校用 USB メモリや外付けハードディスク等の外部記録媒体については、施錠可能な保管庫等で保管しましょう。**
- **外部記録媒体を適切に管理・使用するために管理台帳と使用簿を作成しましょう。**

10. USB メモリ等外部記録媒体の廃棄について

不要になった USB メモリや外付けハードディスク等の外部記録媒体を廃棄する場合、学校情報の漏えいを防ぐため、ハードディスク等の記憶装置から情報を完全に消去する必要があります。

（ 種類別廃棄方法一覧 ）

機器及び記録媒体		消去時期	手順（消去～廃棄）
端末機（ハードディスク） ※教育研修課へ連絡して、廃棄を依頼します~~する~~。		リプレース 又は廃棄時	①ソフト的にフォーマット処理を行います~~おこなう~~。 ②導入業者又は廃棄処理業者へ引き渡します~~す~~。 （廃棄証明の発行要求）
USBメモリ		廃棄時	データ消去後、物理的に破壊して学校で処分してください。
SDカード	書画カメラ用 テレビ用 デジタルカメラ用 ビデオカメラ用	廃棄時	
MOディスク		廃棄時	
フロッピーディスク			
DVDディスク CDディスク			

実施手順

- **不要になった USB メモリや SD カードなどは、データを消去してから廃棄しましょう。**
- **教育内部系~~（校務用）~~端末（校務用端末）や教育外部系~~（授業用）~~端末（授業用端末）、1人 1台端末は、教育委員会の備品になります。故障等あれば学校~~園~~へルプデスクや教育研修課へ連絡しましょう。**

１１．ID・パスワード（認証キー）の管理について

コンピュータは、ICカードのIDとパスワードの認証によってアクセス制限が行われています。

パスワードの管理については、次のようなことが考えられます。

１．パスワードは8桁以上を目安に文字、数字、記号を組み合わせて作成し、ID番号や名前、生年月日等から類推することが困難な文字列としなければならなりません~~い~~。（例えば、かな入力のキー配置を利用して、ある言葉を入力するとランダムな英数文字の組み合わせになります。~~意味はないが発音できる言葉などであれば覚えやすい。~~）

２．パスワードをメモした紙を紛失した等、パスワードが流出したおそれがある場合は、速やかにパスワードを変更しなければならなりません~~い~~。

３．パスワードは定期的に変更し、過去に使用したことのある文字列を再使用してはいけません。~~ならない~~。

実施手順

- **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ようにしましょう。**
- **パスワードは、他人に容易に知られないよう気を付けましょう。**
- **パスワードは定期的に変更しましょう。**
- **席を離れるときはICカードを抜くように心がけましょう。**
- **ICカードのチップは、壊れやすいため丁寧な取扱をしましょう。**

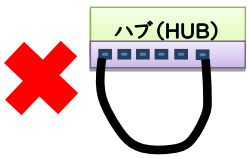
12. ループを起こさないために その①

人事異動等に伴う職員室内のレイアウト変更を行う際に、職員室のLANケーブルの接続を誤り、いわゆる「ループ」と呼ばれる事故が多く発生しています。「ループ」が発生すると、校内のネットワークの速度が異常に遅くなったり、通信不能になったり、ひどい場合は近隣の学校すべてで通信不能になるなど業務に大きな影響がでます。下記の事例を参考に、机の移動などの際、「ループ」を発生させないよう十分な注意が必要です。

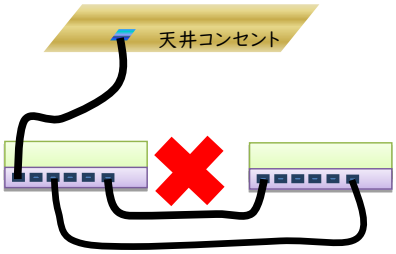
ループとは

ネットワーク内に環状になった部分ができてしまうと、その環状部分でデータ通信が繰り返されてしまい、校内のネットワークの通信データ量が異常に大きくなり、ネットワーク全体の通信が阻害される状態をいいます。

― 職員室内の「ループ」の例 ―



もっとも基本的な「ループ」
使用していないLANケーブルを放置すると、「外れているから」と両端を一つのハブに接続してしまうことがよくあります。この場合、このハブに接続されているコンピュータはほぼネットワークを使用できなくなります。



コンピュータが多い場合、ハブとハブを接続して接続可能なコンピュータ数を増やす場合があります。この場合、LANケーブルは一本だけで接続します。余っているから、二本のほうが早いのではないかと接続するとハブ同士で通信を繰り返し、通信不能になります。

実施手順

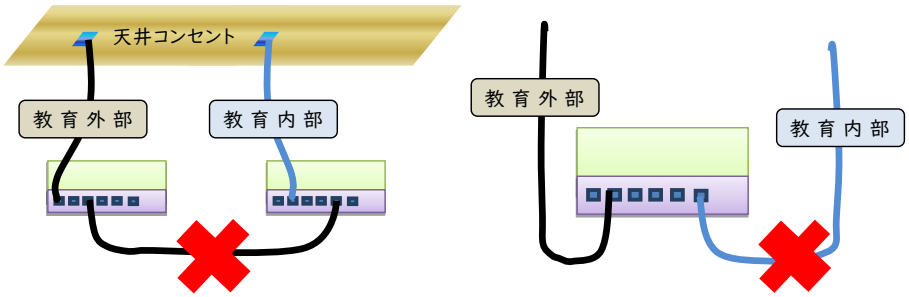
- **職員室のレイアウト変更では、ループの発生を防ぎましょう。**
- **各教職員等のコンピュータはできるだけ移動させないようにしましょう。**
- **職員室内の教育外部系~~（授業用）~~端末（授業用端末）を教室等に持っていく場合にはハブ（HUB）からLANケーブルを外して、LANケーブルごとを移動させましょう。（LANケーブルをハブに残さないように工夫する）**

13. ループを起こさないために その②（ネットワークの混在）

教育内部系（校務用）ネットワークと教育外部系（学習用）ネットワーク

学校には教育内部系と教育外部系の二系統のネットワークがあります。この二つのネットワークは完全に独立しており、混在はありえません。この二系統を一つのハブに接続すると「ループ」となります。この教育内部系、教育外部系が混在した「ループ」は影響が大きく、近隣の学校すべてで通信の異常な遅延が発生します。

― 内部・外部混在の例 ―



実施手順

- **教育内部系のハブと教育外部系のハブ同士を結ぶような接続をしないようにしましょう。**
- **教育内部系（校務用）と教育外部系（学習用）のLANケーブルは絶対に同じハブに接続しないようにしましょう。**

14. 教育内部系（校務用）ネットワークについて

書式変更: 行間 : 1 行

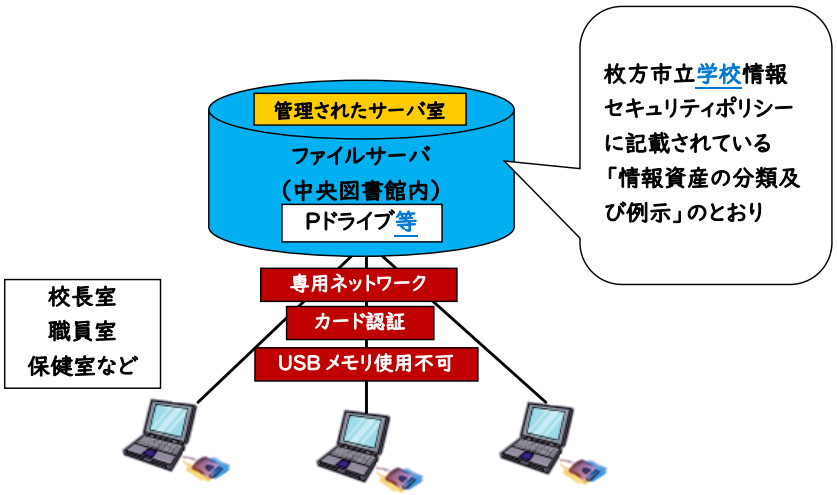
枚方市の教育ネットワークでは、教育内部系（校務用）ネットワーク、~~と~~教育外部系（学習用）ネットワーク及び新~~真~~教育外部系ネットワークがあり、それらはそれぞれ、分離されたネットワークになっています。

≪教育内部系（校務用）ネットワーク≫

情報資産の取り扱いについて~~個人情報~~は、枚方市立学校情報セキュリティポリシーに記載されている「情報資産の分類及び例示」のとおり教育内部系（校務用）ネットワークで扱うものが多くあります。そのため教育内部系（校務用）で扱うデータの保存は、必ずファイルサーバ（Pドライブ）等に保存する必要があります。このファイルサーバは毎日バックアップを取っているので、ファイルが破損したり、間違って削除等してしまったりした場合でも、復元することが可能です（ただし、データ消失直前に戻すことはできません）。しかし、各個人のコンピュータのデスクトップやCドライブ、Dドライブ等に保存していると復元することはできません。

また、デスクトップやCドライブ、Dドライブ等には、保存せず、必ずファイルサーバ（Pドライブ）に保存していれば、万一、コンピュータが盗難に遭ったとしても個人情報が外部に漏えいする危険性は極めて少なくなります。

教育内部系（校務用）ネットワーク



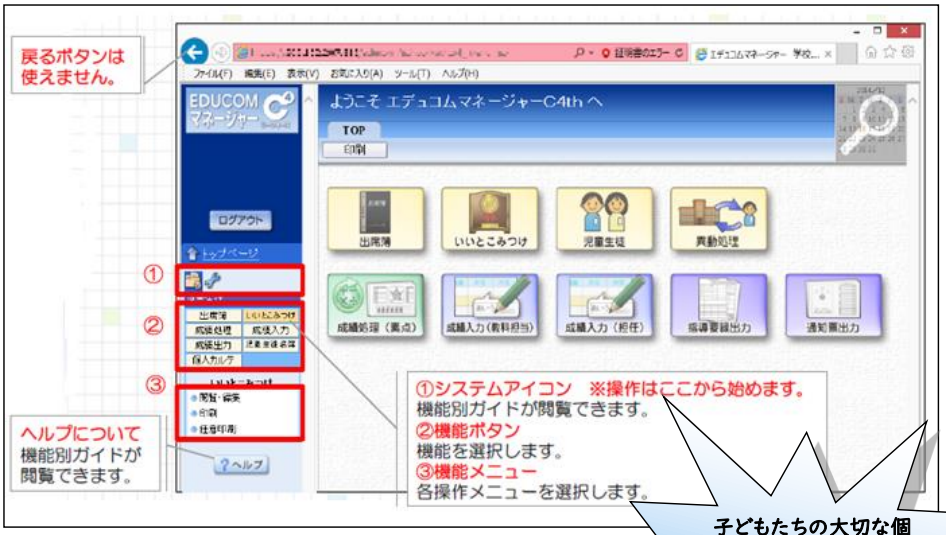
実施手順

- **情報資産の取り扱いは、枚方市立学校情報セキュリティポリシーに基づいて行いましょう。~~個人情報を含むデータは必ず教育内部系（校務用）端末で取り扱いましょう。~~**
- **データは必ずファイルサーバ（学校のＰドライブ等）に保存しましょう。**
- **教育内部系~~（校務用）~~端末（校務用端末）のデスクトップは、整頓して作業しやすいように環境を整えましょう**

○校務支援システム

教職員が児童・生徒と向き合う時間を確保し、よりきめ細かな指導による教育の質の向上を図るとともに、児童・生徒に関する情報を一元管理することで、学校内の情報セキュリティの向上を図るため校務支援システムを導入しています。

校務支援システムでは、児童・生徒の個人情報を取り扱います。したがって、情報漏えいや情報セキュリティには、細心の注意を払うことが必要です。



子どもたちの大切な個人情報です。特に紙媒体での流出には、気をつけましょう。

・席を離れるときはログアウト

児童・生徒の大切な個人情報などが蓄積されていきます。

大切なデータを守るため、席を離れるときはログアウトしましょう。

・長い作業をするときはこまめに保存

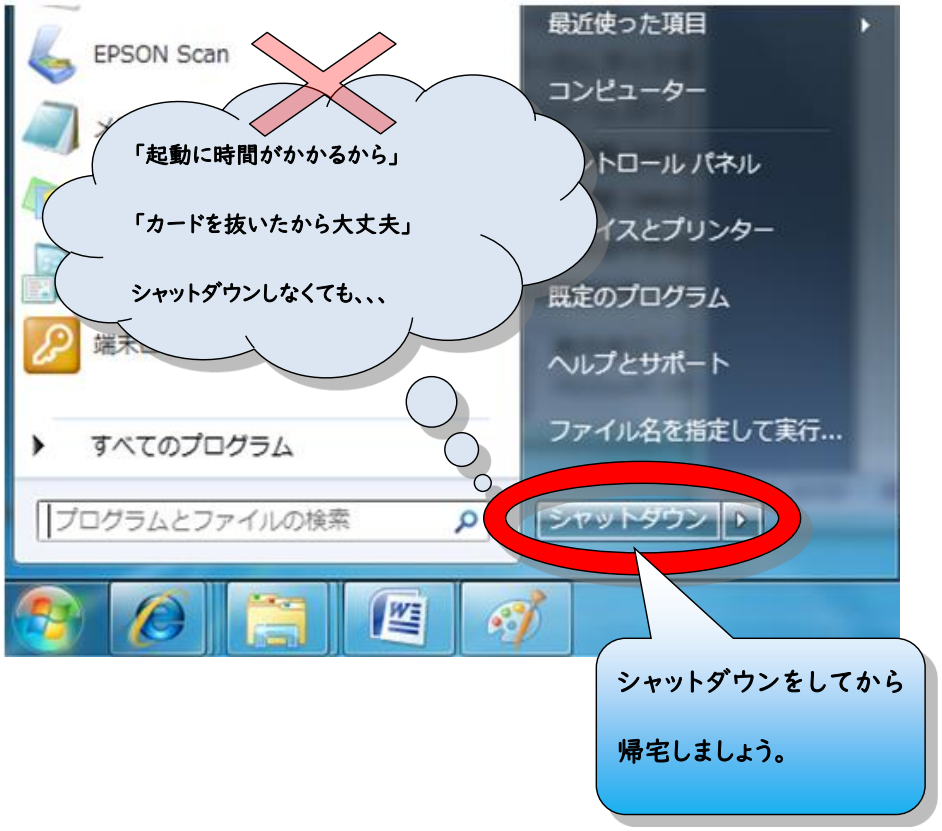
長いメッセージやメールを書いているとき、作業途中で席を離れるときにはこまめに保存をしましょう。30分サーバにアクセスがないとタイムアウトするように設定されています。

実施手順

- **席を離れるときは、ログアウトしましょう。**
- **30分サーバにアクセスがないとタイムアウトになります。作業途中で席を離れるときには、こまめに保存しましょう。**
- **子どもたちの大切な個人情報です。特に紙媒体として打ち出した情報の取り扱い流出には、気をつけましょう。**

〇コンピュータのシャットダウン

「起動に時間がかかるから」「カードを抜いたから大丈夫だろう」といったことでコンピュータをシャットダウンせずに一晩中コンピュータを起動したままにしておくと、知らず知らずのうちにコンピュータ内に不要なデータが蓄積されてコンピュータがフリーズしたり、誤動作したりする等の原因につながります。シャットダウンすることで、コンピュータ内がリセットされますので、帰宅時等長時間使用しない場合は、必ずシャットダウンしなければなりません。



実施手順

- **シャットダウン（再起動を含め）をしてコンピュータ内に蓄積した不要なデータをリセットしましょう。**
- **帰宅時等コンピュータを長時間使用しない場合には、シャットダウンしましょう。**
- **フリーズ等動作が遅いときなど、一度コンピュータの再起動をしましょう。**

○フィルタリングの設定変更

教育内部系~~(校務用)~~端末(校務用端末)において、業務上、閲覧制限されているサイトを利用する必要がある場合には、校内情報セキュリティ責任者(校長)を通じて教育研修課へインターネット閲覧制限解除の依頼が必要となります。

○ソフトウエアのインストール

教育内部系~~(校務用)~~端末(校務用端末)へのソフトウエアのインストールは、インストール依頼書を教育研修課に提出し、教育研修課長が許可したソフトウエアのみインストールが認められます。

・遠隔操作ソフトウエア、ファイル交換ソフトウエア、ネットワーク調査ソフトウエア等のセキュリティ上問題があるものについてのインストールは認められません。
・インストールするソフトウエアごとにインストール依頼書を作成し送付します~~する~~。
・有償のソフトウエアは、ライセンスでコンピュータへのインストール台数が決まっています。インストールを依頼する前に必ずライセンスの確認をする必要があります。

※インストール依頼書は、教育内部系(校務用)ファイル管理フォルダ(Yドライブ)内に保管されているものを利用し、教育研修課へメールにて送付します。
【ファイル管理(Yドライブ)⇒■教育研修課⇒ICT 関係⇒様式集⇒ソフトウエアインストール依頼書】

実施手順

- **ソフトウエアをインストールする前には、依頼書を送付しましょう。**
- **ライセンスにより、コンピュータへのインストール可能台数が決まっているので確認をしておきましょう(例 ライセンス1つにつき1台)。**

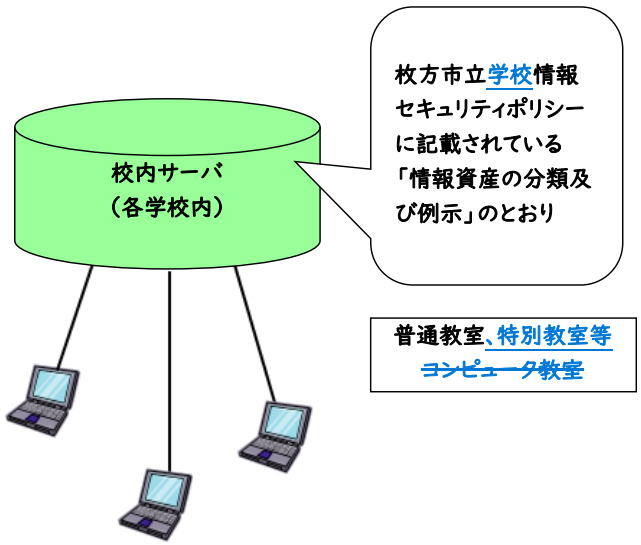
15. 教育外部系（学習用）ネットワークについて

≪教育外部系（学習用）ネットワーク≫

枚方市立学校情報セキュリティポリシーに記載されている「情報資産の分類及び例示」のとおり、教育外部系（学習用）ネットワークコンピュータで扱う個人情報があります。教育外部系（学習用）ネットワークのサーバは、学校内にあります。学校内のサーバには、児童・生徒等の作品や教材等のデータが主に保存されていますが、それら個々のデータ容量は大きく、ハードディスク等の記憶装置の容量も限られているため、不要なデータの削除や使用頻度の少ないものは、DVD等のメディアに保存するなど適切なデータの整理・管理を行うことが必要です。

なお、学校内のサーバにバックアップはありませんが、ファイルの復元機能がありますので、破損等には対応できるようになっています。

教育外部系（学習用）ネットワーク



実施手順

- **教材等のデータは、容量が多いので不要なデータは整理しましょう。**
- **校内サーバには、個人情報を含まない教材等を保存しましょう。**
- **使用頻度の少ないものは、DVD等のメディアに保存しましょう。**

〇コンピュータ教室への入退出管理

コンピュータ教室及び準備室は、学校の情報資産が大量に保管されており、適切な管理が必要です。適切に管理されていない場合には、盗難、損傷等により重大な被害が発生するおそれがあります。

情報セキュリティ上、コンピュータ教室への入退室管理については、使用履歴が分かるように使用簿を作成し、使用者は記入する必要があります。

また、コンピュータ教室を使用しない際は、必ず施錠をして、ネットワークラックの鍵の管理も適切に行わなければなりません。

コンピュータ教室 使用簿例

月/日	時間	学年 クラブ	使用者 （教員名）	教科等	使用ソフト、 ブラウザ等	内容 資料作成、調べ学習等	インターネット 使用の有無
4/10	3限	4-1	鈴木	国語	Word	リーフレット作成	有 ㊙
4/13	5限	6-2	田中	理科	ブラウザ (Edge・Chrome)	調べ学習	㊤ 無

実施手順

- **コンピュータ教室の使用簿を作成し、使用者は記入しましょう。**
- **セキュリティ上、コンピュータ教室を使用しない際は必ず施錠しましょう。**
- **ネットワークラックの鍵の管理も適切に行いましょう。**
- **鍵類の管理と施錠確認は必ず、教職員が責任を持って行いましょう。**

○教育外部系（学習用）校内サーババックアップ

校内サーバ内に保存しているデータは、定期的に光学メディア等にバックアップしておくことで、トラブル時に備えることができます。

特に設置場所が高温になりやすい、夏季はハードディスクが故障する確率が上がるので、
事前にバックアップを行ってください。

◎ICT機器全般に関わる サポートデスク（学校⿊ヘルプデスク）
受付時間 月～金 9:00～12:00、12:45～17:30
TEL 050-7105-8092（内線15-8092）

コンピュータのことで問い合わせる場合、問い合わせ内容と以下のことを伝える。

① 学校名
② 当該職員のカード番号
③ 端末のコンピュータ番号

実施手順

- **教材等のデータは、容量が多いので不要なデータは整理しましょう。**
- **サーバ内は、どこに何があるか分かるように整理しておきましょう。**
- **担当職員で共有や引き継ぎ等できるようにパスワードの適切な管理をしておきましょう。**

○フィルタリングの設定変更

教育外部系~~（学習用）~~端末（授業用端末）で閲覧を禁止するサイトの設定は、「i-FILTER（アイフィルター）」のフィルタリング設定変更でできます。

教育外部系~~（授業用）~~端末（授業用端末）の「i-FILTER（アイフィルター）」設定は、別紙の設定マニュアルを参照してください。

実施手順

- **教育外部系~~（授業用）~~端末（授業用端末）のサイトの制限解除は、校内情報セキュリティ責任者（校長）に了承を得てから行いましょう。**
- **児童・生徒にとって有害（ウイルス感染の危険性が高い）と判断されるサイトについては、ブラックリストに登録し閲覧を制限しましょう。**

○ソフトウエアのインストール

教育外部系~~(授業用)~~端末(授業用端末)へのソフトウエアのインストールは、インストール依頼書を教育研修課に提出し、教育研修課長が許可したソフトウエアのみインストールが認められます。

・遠隔操作ソフトウエア、ファイル交換ソフトウエア、ネットワーク調査ソフトウエア等のセキュリティ上問題があるものについてのインストールは認められません。
・インストールするソフトウエアごとにインストール依頼書を作成し送付する。
・有償のソフトウエアは、ライセンスでコンピュータへのインストール台数が決まっています。インストールを依頼する前に必ずライセンスの確認をする必要があります。

※インストール依頼書は、教育内部系（校務用）ファイル管理フォルダ（Yドライブ）内に保管されているものを利用し、教育研修課へメールにて送付。
【ファイル管理（Yドライブ）⇒■教育研修課⇒ICT 関係⇒様式集⇒ソフトウエアインストール依頼書】

実施手順

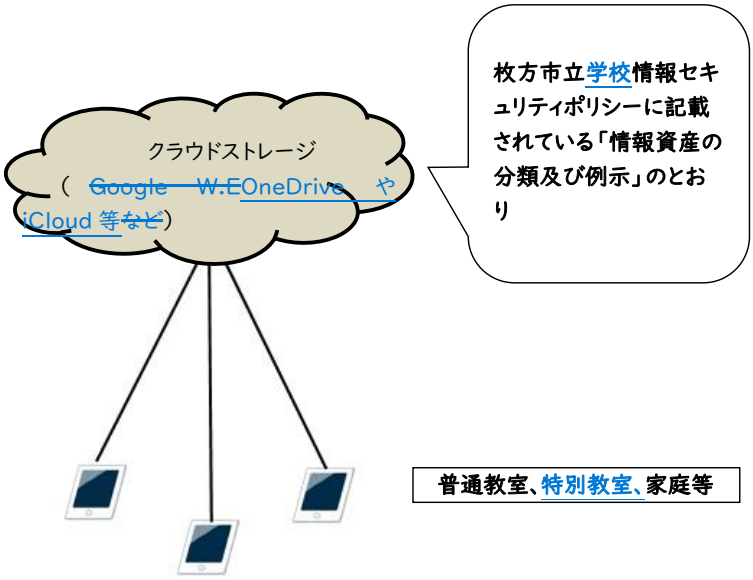
- **ソフトウエアをインストールする前には、依頼書を送付しましょう。**
- **ライセンスにより、コンピュータへのインストール可能台数が決まっているので確認をしておきましょう（例 ライセンス1つにつき1台）。**

16. 新教育外部系ネットワークについて

≪新教育外部系ネットワーク≫

新教育外部系ネットワークでは、児童・生徒、教職員が1人1台端末を取り扱う際~~授業支援~~に用いるネットワークになり、児童・生徒の課題等は、新教育外部系ネットワークコンピュータで扱います。新教育外部系のデータは、1人1台端末に保存できるだけでなく、クラウドストレージに保存することができます。

新教育外部系ネットワーク



書式変更：中央揃え

実施手順

- データを1人1台端末本体には保存せず、クラウドストレージに保存しましょう。~~することを心がけましょう~~

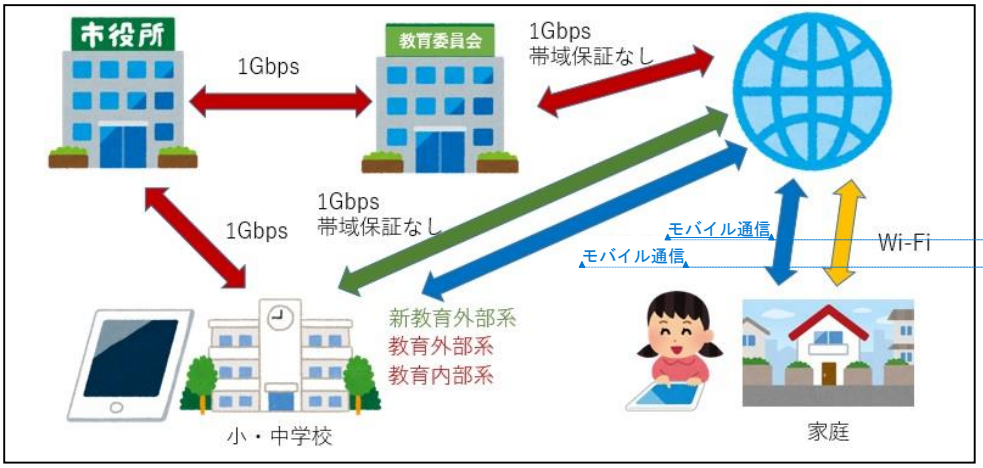
○移動体通信を利用した１人１台端末について

GIGA スクール構想の実現に向け、全学年の児童・生徒一人一人がそれぞれ端末を持ち、十分に活用できる環境の実現をめざす~~目指す~~ため、セルラーモデル ~~LTE~~端末を配備しました。ネットワークの形態については、普通教室や特別教室などに無線 LAN アクセスポイントを整備しており、新教育外部系ネットワークの無線 LAN を利用できます。

無線LANアクセスポイントがないグラウンドや校外学習などにおいても、モバイル~~LTE~~通信回線を使用することができ、家庭においても~~持ち帰り~~学習で~~に~~活用できます。家庭に持ち帰る際には、注意事項やルールを定め、児童・生徒が正しく安全に １ 人 １ 台端末を利用することができるようにする必要があります。また、各学校においては、児童・生徒に対して教職員が情報モラル教育やデジタル・シティズンシップ教育を行うこと、定期的に教職員、児童・生徒に貸与した １ 人 １ 台端末数の確認、管理を行う必要があります。

書式を変更: フォント : (英) UD デジタル 教科書体 NK-R, (日) UD デジタル 教科書体 NK-R, (特殊) +本文のフォント - 日本語 (MS 明朝)

<セルラーモデル ~~LTE タブレット~~端末の利用イメージ>



書式を変更: フォント : 9 pt

書式を変更: フォント : (英) MS ゴシック, (日) MS ゴシック, 9 pt, フォントの色 : テキスト 1

書式変更: 中央揃え

書式を変更: フォント : 9 pt

書式を変更: フォント : (英) MS ゴシック, (日) MS ゴシック, 9 pt, フォントの色 : テキスト 1

書式変更: 中央揃え

１人１台盗難防止対策等

・教室から離れる場合は、部屋の施錠をする。(児童・生徒機)

・職員室では端末を使用しない時は、鍵のかかる引き出しなどに保管する。(教職員機)

・定期的に端末を確認する。

○フィルタリングの設定変更

１人１台端末の「i-FILTER（アイフィルター）」設定解除は、校長が承認する場合、教育研修課に依頼してください。

実施手順

- **新教育外部系のインターネット閲覧制限解除は、校内情報セキュリティ責任者（校長）に了承を得て 教育研修課~~（ICT 推進 G）~~に依頼して下さい 。**
- **児童・生徒にとって有害（ウイルス感染の危険性が高い）と判断されるサイトについては、ブラックリストに登録し閲覧制限を行います。~~しましょう。~~ この場合も校内情報セキュリティ責任者（校長）から教育研修課~~（ICT 推進 G）~~に依頼して下さい。**

○ソフトウエアのインストール

１人１台端末にインストールできるソフトウェア（アプリ）は、枚方市教育委員会が検証し、学校情報セキュリティ管理者が認めたものに限ります。使用できるアプリは枚方版アプリストア「セルフサービス」に格納されています。~~ので、授業等で必要なアプリをインストールしたい場合は、枚方市教育委員会 ICT 教育ポータルサイト「GIGAスク!ひらかた」「枚方版アプリストアの運用について」を参照してください。~~

実施手順

- **~~枚方版アプリストア~~「セルフサービス」の中から必要なアプリをインストールできます。**
- **アプリをインストールしすぎると端末本体のストレージがいっぱいになりますのでご注意ください。**

○パスコードの変更

１人１台端末のパスコードについては、児童・生徒の発達段階に応じて適切に変更する必要があります。別紙１「児童・生徒用１人１台端末のパスコード設定（例）」を参照してください。教職員の端末についても、定期的なパスコードの変更が必要です。

実施手順

- **児童・生徒の発達段階に応じた適切な変更を、定期的に行ってください。**

〇その他取り扱いの注意

教職員に配備された１人１台端末は、原則枚方市立小中学校で常勤する間は学校が異動になっても引き続き使用できます。大切に使いましょう。

児童・生徒の１人１台端末については、学校在校中は引き続き使用できますが、児童・生徒が転校する際は従前の学校で回収となります。一方、年度途中で転入生があった場合は、予備機を配備してください。

令和７年の端末更新までは、教職員の端末に故障や破損があった場合は、直接 NTT ドコモヘルプデスク（0120-541-099）に問い合わせしてください。端末更新後は、教育研修課に連絡してください。

児童・生徒の端末に故障や破損があった場合は、教育研修課~~（ICT 推進 G）~~に連絡し、破損や故障の状況を伝えてください。状況に応じて対応することになります。

万が一、紛失し行方不明となった場合は、直ちに教育研修課~~（ICT 推進 G）~~に連絡してください。当該端末に対して遠隔でロックをかけるとともに、電波を検知できれば大まかな場所がわかります。

キーボード付ケースについては、自然故障の補償期間があります~~令和５年12月までとなっています~~。自然故障した場合は、キーボード付ケースを教育研修課~~（ICT 推進 G）~~に持参~~送付~~し、学校にある予備機のキーボード付ケースで対応してください。

１人１台端末の充電器、充電ケーブルは消耗品です。破損や故障した場合は、予備機の充電器などと交換し、必要があれば、学校で購入してください。また、学校で充電器・充電ケーブルを購入する際は、純正品または MFi 認証の~~それに準ずる~~ものを購入するようにしてください。

実施手順

- ~~１人１台端末（児童生徒機）→教育研修課（ICT 推進 G）で対応~~
- ~~１人１台端末（教職員機）→NTT ドコモヘルプデスク（0120-541-099）で対応~~
- **紛失し行方不明となった場合は、直ちに教育研修課~~（ICT 推進 G）~~に連絡**
- **キーボード付ケースの自然故障は補償対象→教育研修課へ持参~~（ICT 推進 G）で交換~~**
- **充電器、充電ケーブルは消耗品→学校で購入**

別紙１

児童・生徒用１人１台端末のパスコード設定（例）

発達段階に応じたパスコードの設定と、情報モラル教育、デジタル・シティズンシップ教育を実施

低学年：**保護者と一緒にパスコードを決め、設定**。

・パスコードは全員異なるものであることを知る。

・パスコードは他人に知られてはいけないことを知る。

高学年：**4桁の数字を児童が自分で考え、パスコードを設定**。

・パスコードは他人に推測されないものが良いことを知る。

中学生：**6文字以上、英数字のパスコードを生徒が自分で考え、設定**。

・パスコードは英数字や大文字小文字を使用し、
複雑なものであるほうが良いことを知る。

※小学校においても、設定の変更でパスコードを数字4桁から英数字6桁以上に変更することが可能です。

※上記はあくまでも一例です。学校の状況に応じてパスコードの設定を行ってください。ただし、全員が同じパスコードにならないようにしてください。また、初期パスコードのままで使用しないように注意してください。

（参考 HP）
はじめてのパスワード指導：文部科学省
https://www.mext.go.jp/studxstyle/skillup/1.html