前橋市立学校　教職員用コンピュータ利用規程

平成２７年１０月１日　前橋市教育委員会

（目 的）

１　本利用規程の目的

本利用規程は、前橋市立学校教職員用コンピュータ（以下「教職員用ＰＣ」という ）の利用について規定するものであり、教職員用ＰＣを利用する者（以下「利用者」という）は、個人情報の保護及び情報セキュリティの保持のために本利用規程を遵守しなければならない。

２　教職員用ＰＣの定義

教職員用ＰＣは、学校教育の目標及び学校の教育目標の達成のために校務や授業等で利用する、デスクトップ型、ノート型、タブレット型等の各種ＰＣとする。また、学校が独自に導入したＰＣも含める。

（管理者）

１　管理責任者

各学校の教職員用ＰＣの管理責任者（以下「管理者」という ）は、校長が務める。

２　運用責任者の設置

管理者は、教職員用ＰＣの運用責任者を任命し、教職員用ＰＣの活用に関わる業務にあたらせる。運用責任者の主な業務は、教職員用ＰＣの技術的な設定及び運用とする。

３　管理者の業務

(1) 教職員用ＰＣの管理

管理者は、別記様式１のリース物品管理台帳（ 以下「管理台帳」という ）を定め、利用者に教職員用ＰＣを貸与させることができる。また、学校が独自に導入したＰＣについても、学校で作成した管理台帳により、同様の扱いをする。

管理者は、教職員用ＰＣのネットワークへの接続設定のための、ＩＤ及びパスワードを利用者に付与するとともに、ソフトウェアのインストールなどの記録及び利用履歴を管理台帳で管理しなければならない。

(2) 利用規定の遵守

管理者は、利用者に対し、本利用規程を遵守させなければならない。本利用規程を遵守しない利用者に対し、教職員用ＰＣの利用停止もしくは、利用を制限する権限を有する。

(3) ウィルス情報などの提供

管理者は、利用者に対し、ウィルス情報、アップデート情報等を提供しなければならない。

(4) データの保守

管理者は、職員室に設置されている画像・映像等保存用サーバ（以下「画像サーバ」という）及びデータセンター内に設定された自校の保存領域（以下「データセンター」という）に保存されたデータの保守業務に努めなければならない。

（個人情報の保護）

１　関連例規の遵守

個人情報の保護及びその取扱にあたっては、前橋市個人情報保護条例及び前橋市情報セキュリティポリシー、前橋市教育委員会個人情報保護のガイドラインを遵守しなければならない。

２　教職員用ＰＣの持ち出し

教職員用ＰＣは、所属校の校内でのみ使用できるものとし、校外への持ち出しは禁止する。ただし、遠足や社会科見学等の校外学習で使用する場合や、市内教育関係団体・ＰＴＡ等の各種事業に供する場合は、管理者の許可を受ければ、所属校の校外であっても使用することができる。

（情報セキュリティの保持）

１　情報セキュリティの保持義務

利用者は、教職員用ＰＣの正常な動作を維持し、情報セキュリティを保持するために、以下の項目を遵守しなければならない。

(1) アップデート

利用者は、ＯＳやソフトのセキュリティアップデート等を定期的に行い、最新の状態に保つこととする。ただし、ＯＳやソフトのバージョンは、必ずしも最新でなくてもよいこととする。

(2) ウィルス対策

利用者は、ウィルス対策ソフトのパターンファイルを最新の状態に保ち、定期的にウィルスチェックを行うこととする。また、教職員ＰＣ以外のＰＣで作成したデータをデータセンターまたは画像サーバに保存する際には、当該データについてウィルス検査を実施し、安全を確認しなければならない。

(3) 守秘義務

利用者は、ネットワークに接続するために必要なＩＤ、パスワード等の諸情報の機密について、守秘義務を負うものとする。

(4) 緊急時の対応

利用者は、ウィルス感染等の緊急時の場合、速やかに管理者に報告し、指示を仰ぐこととする。

２　データの保存

(1) 利用者によるデータの保存

利用者は、作成したデータを保存する場合、その種類に応じてデータセンター、画像サーバのいずれかに保存しなければならない。ただし、重要な個人情報や重要なデータは、必要に応じ、暗号化した上で、外付けハードディスクやＣＤ－Ｒ等の外部記録媒体に保存して金庫等に保存する等、適切な措置を講じることとする。

(2) データの種類および保存先

校務で利用されるデータを次の４種類に分類し、保存先を限定する。

ア　重要な個人情報が含まれるデータ

児童生徒の学籍や成績、身体測定の記録など守秘義務を要する重要な個人情報が記載されているデータ。保存先は、データセンターとする。

イ　個人情報が含まれるデータ

学習指導案や学級通信など児童生徒の写真や氏名などが記載されているデータ。保存先は、データセンターとする。

ウ　個人情報は含まれないが、学校運営に必要なデータ

各分掌が校務で使用しているデータ。保存先は、データセンターとする。

エ　個人情報の有無に関わらず、多くの容量を消費するデータ

学習用ソフトや画像、行事写真・映像などのデータ。保存先は、画像サーバとする。

(3) データセンターへの保存ルール

上記ア、イ、ウのデータをデータセンターに保存する際は、別紙１で示す保存ルールに従うこととする。

３　データの管理

(1) 定期的なデータ管理

管理者は、データセンター内のデータが保存ルールに基づいて保存されているか定期的に確認し、必要に応じてデータ移動等の管理作業を行うこととする。

(2) データの持ち出し禁止

データの種類によらず、校内で作成したデータの複製及び校外への持ち出し行為を禁止する。ただし、データの種類イ、ウ、エについては、管理者の許可を受ければ持ち出すことができる。

(3) データ複製及び校外への持出し時の遵守事項

データの複製及び校外への持出し行為を管理者に許可されたデータの種類イ、ウ、エに関しては、以下の事項を遵守する。

ア　データは個人情報を記号等に置き換えた上で、暗号化やパスワードによるロックなどの適切な措置を講じ、外部記録媒体（ＵＳＢメモリー等）を通して複製すること。

イ　データを校外に持出す場合は、別記様式２の管理簿等に持出す事由や持出し期日等、必要事項を記入し、管理者の許可を得ること。

ウ　データを複製した外部記録媒体を持ち運ぶ際は、常に身につけ、盗難や紛失のないよう十分な管理を行うこと。

エ　データを複製した外部記録媒体は、私用のデータを保存してある外部記録媒体と分けるなどして、十分な管理を行うこと。

オ　データを保存した外部記録媒体を廃棄する際は、物理的に破壊するか専用のソフトを用いてデータを完全に削除すること。

カ　自宅等でデータを使用する場合は、複製したデータがインターネット等を通して漏洩することがないよう、自宅等のコンピュータのセキュリティを教職員用ＰＣと同等以上に保持すること。特に、ウィニー等のファイル交換ソフトのインストールされているコンピュータやウィルス対策ソフトが最新版に更新されていないコンピュータでの使用

は禁止する。
キ　自宅等でデータを更新した場合、データは自宅等のコンピュータ等に保存しないこと。
ク　持ち出したデータが盗難や紛失した場合や、インターネット等を通じて漏洩した場合、速やかに管理者に報告し、指示を仰ぐこと。

(4) インターネット上で企業が運営するストレージサーバ等の利用

インターネット上で企業が運営するストレージサーバや電子メールへの添付などについてもデータの複製及び持出し行為と同様の扱いとする。

（公序良俗に反する行為の禁止）

１　私的利用の禁止

教職員用ＰＣの私的利用は禁止する。職務に関係のない Web ページの閲覧やインターネットサービスの利用、私有メールアドレスの利用及び私的メールの送受信、私的データの保存については禁止する。

２　違法ソフト等のインストール禁止

教職員用ＰＣの利用にあたって、正規ライセンスを所有していない違法ソフト及び校務処理ソフト、利用目的に関係のないソフトをインストールすることは禁止する。

（設定の変更等）

１　初期設定の変更

教職員用ＰＣの設定は、校務に支障のない限り、マウスの設定の変更等、簡易な変更について認めることとする。

２　ソフトウェアのインストール

校務を円滑に進める上で必要な場合は、必要最小限のソフトウェアを教職員用ＰＣにインストールすることができる。この場合、管理者の許可を受け、管理台帳に記載しなければならない。さらに、当該ソフトの使用許諾契約に反しない方法でインストールすることとし、当該ソフトの著作権を遵守することとする。

３　周辺機器（ハードウェア）の追加

教職員用ＰＣに係る周辺機器の追加は、原則禁止する。ただし、校務を遂行する上で必要な場合は、管理者の許可を受けて追加することができる。この場合、管理台帳に記載しなければならない。

４　返納の際の初期化

異動等で利用者が教職員用ＰＣを返納する際には、設定の変更箇所をすべて初期化し、管理者に確認を求めることとする。

５　責任の所在

上記４項の初期設定の変更によって何らかの問題が生じた場合は、利用者本人がその責任を負う場合がある。

（個人所有コンピュータの取り扱い）

１　個人所有コンピュータ等の持ち込み禁止

個人が所有しているコンピュータ等（以下「個人所有ＰＣ」という）を校内に持ち込む行為は、これを禁止する。

２　例外措置

個人所有ＰＣの持ち込みが、校務や授業を遂行する上で必要な場合は、管理者の許可を受けて、校内に持ち込み、これを使用することができるものとする。ただし、以下の事項を遵守すること。

(1) 個人所有ＰＣを校内ＬＡＮに接続しないこと。

(2) 個人所有ＰＣへのデータ等の複製については、本規程の個人情報の保護におけるデータの保存及びデータの複製に準ずること。

（附 則）本利用規程は、平成１８年　４月１日から施行する。

（附 則）本利用規程は、平成２５年　４月１日から施行する。

（附 則）本利用規程は、平成２７年１０月１日から施行する。

様式１

リース物品管理台帳

No.

１ リース物品の記録

種 別		メーカー	
型 番		付属品	
本体表示		備 考	

２ リース期間の記録

導入年度	リース期間	納入年月日	管理職印
	～	． ．	

３ リース期間中の管理

年月日	使用場所	使用者	摘 要	使用者印
． ．				
． ．				
． ．				
． ．				
． ．				
． ．				
． ．				
． ．				

４ リース満了後の管理

年月日	使用場所	使用者	摘 要	使用者印
． ．				
． ．				
． ．				
． ．				
． ．				

５ 廃棄等の記録

年月日	廃棄等処理	管理職	摘 要	管理職印
． ．	廃棄 ・ 移動			

様式２

学校データ持ち出し管理簿

学校名	

持　出 年月日	返　却 年月日	持出データ名称	持出の事由	持出者氏名	持　出 確認印	返　却 確認印

別紙１

MENET データセンター保存ルール

１　MENET データセンターに保存しなければならないデータ

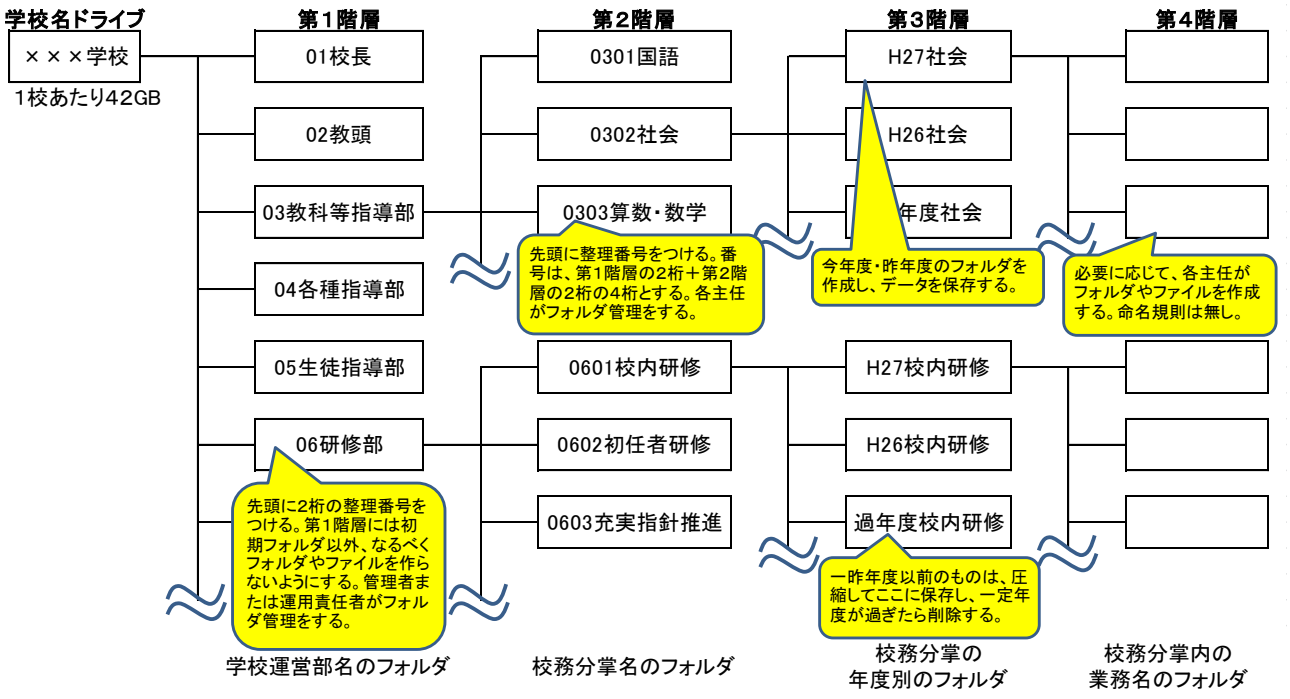
ア　重要な個人情報が含まれるデータ（児童生徒の学籍や成績、身体測定の記録など）
イ　個人情報が含まれるデータ（学習指導案や学年・学級通信など）
ウ　個人情報は含まれないが、学校運営に必要なデータ（各分掌の校務データなど）

２　MENET データセンターに保存できない校務データ

エ　個人情報の有無に関わらず、多くの容量を消費するデータ
（学習用ソフトや画像、行事写真・映像のデータなど）

３　フォルダ・ファイルの整理

各校の分掌組織図を元にしたフォルダ構造を作成し、データを整理して保存する。
以下に、フォルダ構造及びフォルダ名の例を示す。



（１）第１階層フォルダ（学校名ドライブのダブルクリックで最初に見えるフォルダ）
「01●●」～「16●●」のように、先頭に２桁の整理番号をつけ、その後に学校運営部の名前を付けたフォルダ名にする。

（２）第２階層フォルダ（「0302 社会」のようなフォルダ）
「XX01●●」～「XX20●●」のように、上位フォルダの整理番号（XX）に第２階層の整理番号２桁をつけ、その後に校務分掌の名前を付けたフォルダ名にする。

（３）第３階層フォルダ（「H27 社会」のようなフォルダ）以下
年度ごとのフォルダを作成し、当該年度のファイルを保存していく。必要に応じて、第４階層以下にフォルダやファイルを作成していく。

４　留意事項

（１）データセンターはデータ消失等のリスクに対する高い安全性が保証されているため、重要データは必ずデータセンターに保存する。

校内の教職員による人為的なミスについては、誤って削除してしまってもゴミ箱機能により復活できる場合がある。ただし、誤って上書きしてしまった場合は復活できない。（そのため、消失が許されない重要なデータは、暗号化した上で外付けハードディスクやＣＤ－Ｒ等の外部記憶媒体に保存して金庫等入れておく等、適切な措置を講ずる必要がある。）

（２）各学校に割り当てられているデータセンターの保存領域（一律４２ＧＢ）を使い切ってしまわないよう、日常的に使用済容量をチェックし、必要な措置を講ずる。

〔措置の例〕

①使用済容量が４０ＧＢを超えたら、古いフォルダやファイルの削除、外部記憶媒体へのバックアップなどを呼びかける。

（限度付近まで使い切ってしまうと、緊急時に保存できないなどの不具合が生じるため）

②フォルダごとの使用容量をチェックし、大きいフォルダの担当者に整理を呼びかける。

③画像や映像等のデータが保存されている場合には、フォルダ担当者に対して画像サーバへの移動を促す。または担当者の許可を得て移動する。

（３）デジタルカメラ等で撮影した写真や映像データは非常に大きいため、データセンターへの保存は行わず、必ず職員室にある画像サーバへ保存する。また、画像や映像を貼り付けた文書データ（学年・学級便り、プレゼン資料など）もデータが非常に大きくなっている場合があるため、その際は画像サーバへ保存する。

（４）職員室にある画像サーバは２重のバックアップ体制で運用されるが、管理状況によってはデータ消失のリスクも存在するため、必要ならば以下の措置を講ずる。

〔措置の例〕

①画像サーバの稼動状態をステータス画面で日常的にチェックし、不具合が発生している場合には速やかにヘルプデスクに連絡する。

②画像サーバに保存した画像や映像などのうち、消失が許されないものについては、外部記憶メディア（外付けハードディスクやＣＤ－Ｒなど）にバックアップしておく。

③画像サーバの設置場所に注意し、日常的なチェックをしにくい場所やホコリが多い場所、直射日光が当たる場所などは避けるようにする。また、盗難防止のチェーンロック、無停電電源装置（ＵＰＳ）を確実に接続しておくようにする。