別冊1

美瑛町立小中学校　情報セキュリティ・ポリシー

美 瑛 町 教 育 委 員 会

令和３年３月１日　策定

(令和３年４月１３日 一部改正)

Ⅰ　基本方針

1　はじめに

企業と同様に学校にも、人・物・金・情報の４つの財産があるが、近年のインターネット・イントラネットなどの情報システム・ネットワークの著しい発展に伴い、情報の重要性は加速度的に高まってきている。本町の小中学校においても、情報の有効活用なしには円滑な教育活動の推進は望めない。

その一方で、多くの教育現場において、コンピュータウイルスや不正アクセス、記録メディアの盗難による改ざんや破壊、紛失、機密漏洩等の問題が発生している。こうした問題が発生すると、情報資産の直接的な損失のみならず、信用の失墜や、場合によっては損害賠償などの副次的な損失を被る可能性がある。

今日の情報化社会において、学校も教育活動のさらなる充実を目指し、保護者や地域社会の信頼を得るためには、職員各自が取り扱う情報の重要性を十分認識し、その保護に努めなければならない。そのため、情報セキュリティの向上を重要な施策の一つとして実施する必要がある。

2　目的

（１）本町の小中学校における情報資産を保護し、校務を円滑に推進するための基本的な考え方や体制、規則について定めるものとする。

（２）本セキュリティ・ポリシーを職員間に徹底し、適切なセキュリティ対策を施すことで、各学校におけるセキュリティ・レベルを向上させるとともに、保護者や地域社会の信頼を高める。

3　組織

●各小中学校では、教頭のほか、教職員からなる「教育情報セキュリティ管理委員会」を設置し、各校のセキュリティを維持・管理・運営する。

●教育情報セキュリティ管理委員会の運営に関する管理責任者として、「教育情報セキュリティ管理者」を置き、校長がこれにあたる。

●教育情報セキュリティ管理委員会の構成員の任期は原則として１年とする。

4　適用対象者

●本セキュリティ・ポリシーは、各小中学校の全教職員（以下、「教職員」という）に対して適用される。

●情報資産の利用に関して外部に委託する場合も、本セキュリティ・ポリシーを周知すること。

●児童生徒に対しては、情報リテラシー※１を必要とする時間に、情報社会に参画する上での基本的な考え方や態度を指導すること。

※１）情報リテラシー
情報機器やネットワークを活用して、情報やデータを取り扱う上で必要となる基本的な知識や能力のこと。
IT の世界で単に「リテラシー」というと、通常「情報リテラシー」のことを指す。

5　適用範囲

各小中学校が所有するすべてのサーバ・クライアント PC および周辺機器、並びにそれらで扱う全ての情報を対象とする。

また、印刷物など二次的に生産されたものにも適応される。

（１）情報資産の分類と管理方法

①　ねらい

・児童生徒及びその家庭が被る可能性のある脅威の芽を未然につむために、個人情報の漏えいを防ぐ

・教職員の業務推進の著しい妨げを防ぐ

②　情報の種類分け　※「個人情報に該当しないもの」、また、「写し」を含む

区分	内容	具体
S	持ち出してはならないもの ①児童生徒に関すること	①指導要録　②卒業台帳 ③児童生徒の異動に係るもの　④健康診断票
	持ち出してはならないもの ②教職員に関すること	①人事情報　②職員台帳情報　③家庭環境情報 ④保健情報　⑤その他個人が特定される情報
A	①児童の家庭環境が明らかになるもの	①家庭環境調査書　②児童生徒名簿　③学級連絡網 ④集団下校名簿　⑤健康調査票 ⑥連絡メール等の登録者名簿
	②児童の成績に関するもの	①通知表（一覧表及び下書きを含む） ②テスト等の結果をまとめたもの
	③特定の児童の様子及び行動が明らかになるもの	①事故報告書又はこれに準ずるもの　②すとりーむ ③個別の指導計画　④出席簿及び健康観察票
B	①児童が本校に在籍していることが明らかになるもの	①児童生徒の氏名及び顔写真が掲載されている学校及び学年、学級通信　②児童生徒名簿（氏名・学年・学級のみ）
	②児童個人の学習の状況が明らかになるもの	①テスト　②ワークシート　③ドリル ④児童生徒が作成した作品等
	③その他	①各校務分掌に関わる文書
C	上記外	①授業に使用する資料　②児童生徒の氏名及び写真が掲載されていない学校及び学年、学級通信

③　情報等管理の方策

共通	●情報資産については、使用者がいない教室及び職員室机上への放置を行わない。 ●印刷物については、所定の場所で管理し、保存年限の経過したものは、担当者が必ず処分を行うこと。 ●学校 PC 以外でデータ作業を行う場合は、ウイルス対策ソフトが入っていない媒体の使用を禁止する。 ●ペーパーの処分（古紙、裏紙等）についても、同様に留意すること。
S	●職員室外への持出しを一切禁止する。
A	●データの持ち出しについては、事前に申請し、校長の承認を得た USB を使用し、適切に管理すること。USB の保管については、職員室の施錠可能な場所とする。 ●ペーパーの持ち出しについては、校長又は教頭の許可を得て、常に携行すること。また、必要がなくなったものについては，必ずシュレッダーで処分をすること。 ●通知表等については、一覧から児童生徒氏名を抜いたものを使用する。
B	●データの持ち出しについては、事前に申請し、校長の承認を得た USB を使用し、適切に管理すること。USB の保管については、職員室の施錠可能な場所とする。また、クラウド（Google ドライブ）による持ち出しについても、事前に申請の上、持ち出すこと。以上のことを踏まえ職員室外への持ち出しを認める。 ●持ち出したペーパーは，常に携行すること。 また、必要がなくなったものについては、必ずシュレッダーで処分をすること。 ●学校及び学年、学級通信について、児童生徒の写真の貼付や氏名の入力は、原則、職員室で行うこと。 また、児童生徒の写真にその氏名を添付しないことや、生年月日を記載しないよう留意すること。
C	●適切な管理を行う。

6　適用対象者の義務

（１）遵守の義務

教職員は、情報資産の取り扱いに際して、本セキュリティ・ポリシーおよび情報セキュリティに関する各種規定を順守すること。当該規定の追加・変更などの通達があった場合には、直ちに内容を確認すること。

（２）守秘義務

教職員は、職務上知り得た情報を、職務上必要な場合を除き、第三者に開示・提供・漏洩してはならない。また、開示する場合の内容は必要最小限とすること。

（３）説明の義務

情報管理委員会は、本セキュリティ・ポリシーに追加または変更等が行われた場合には、直ちに適応対象者に通知するとともに、必要に応じて説明を行うこと。

教育情報セキュリティ管理委員会は、本セキュリティ・ポリシーに関する質問や意見に対し、速やかに対応すること。

Ⅱ　情報資産の取扱

1　目的

（1）各小中学校が所有するコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体及び情報が印刷された文書等（以下、「コンピュータ等」という。）の正しい取り扱い方法を明確にし、ハードウェア、ソフトウェアデータ等の情報資産を保護すること。

（2）コンピュータ等の取り扱いに関して想定される以下のような問題の発生を防ぐこと。

① コンピュータ等の取り扱いミスによる物理的な破壊、故障、盗難、紛失等。

② コンピュータ等の操作ミス、取扱ミスによる重要データの消失、破壊、漏洩等。

③ コンピュータ等の設定ミス及び保管ミスによるセキュリティ・レベルの低下。

④ 情報資産を扱う意識の欠如による情報の消失、破壊、漏洩等。

2　基本規定

（1）管理者

各小中学校が所有するコンピュータ等は、すべて教育情報セキュリティ管理者が管理責任を負う。

（2）管理の義務

① 教職員は、自らが使用するコンピュータ等を管理する義務を負う。

② 学習活動等で情報機器等を児童生徒に使用させる場合は、児童生徒が適切な使用をしているか管理・監督する義務を負う。

③ 支給以外のコンピュータ等の学校への持込使用は原則禁止とする。ただし、業務上必要な場合は、教育情報セキュリティ管理者の許可を得て使用することができる。

（3）日常校務における取り扱い

① 日常校務において使用するコンピュータ等の取り扱いや設定に関しては、教育情報セキュリティ管理委員会の指示に従うこと。

② コンピュータ等は、常に所定の、かつ安全な場所に設置して使用し、落下、激突、塵、水分、熱等による破損や故障から保護すること。

③ 情報機器を帰宅時および長時間使用しない場合には、電源を切り、不特定多数が閲覧できないよう適した場所に保管すること。ただし、正当な理由があって電源を切ることができない、または適切な場所に保管できない場合には、ディスプレイの電源を切るなどの措置をとること。

④ 校務に無関係なソフトウェアを使用し、情報を検索・閲覧をしないこと。

⑤ 情報資産を扱っているという意識を常に持ち、重要度に合わせて適切に扱うこと。重要情報を児童生徒が閲覧可能な場所に保存しないこと。また、記録されたメディアやパソコン及び情報が印刷された文書等を児童生徒の目につく場所に放置しないこと。

⑥ 学校所有のノート型 PC 及びモバイル端末は、帰宅時や長時間使用しない場合は職員室等の防犯対策がとられている部屋（鍵のかかる場所）に保管すること。

⑦ USB メモリは、教育情報セキュリティ管理者が管理する。また、使用時は貸し出し簿に記入すること。

⑧　在宅勤務や校外研修など、ノート型 PC やモバイル端末、電磁的記録媒体等、重要情報が記録されたメディアを学校外へ持ち出す必要がある場合は、管理職に許可を得て、持ち出し記載簿に記入すること。なお、持ち出しの場合は、退勤時・出勤時において私用のために他の場所に立ち寄ることを禁ずるとともに、盗難・紛失・破損には、十分注意すること。持ち出せる情報については、「Ⅰ　基本方針　5　適用範囲」の（1）を参照のこと。

⑨　情報資産を廃棄する際について、ハードディスクなどの記録媒体は、データを上書き消去または物理的に破壊すること。また、印刷物など二次的に生産されたものは、シュレッダーで処理する。

（4）操作および設定変更

教職員は、美瑛町教育委員会の許可なく、学校が所有するコンピュータに以下で示すような操作および設定変更をしてはならない。

①　ソフトウェアのインストール、バージョンアップ、削除

②　ハードウェアの追加、変更、取り外し。

③　ネットワークに関する設定変更

④　手動によるシステム・ファイルの操作

⑤　スタートアップ・プログラム、メモリ常駐プログラムの設定変更

⑥　手動によるレジストリ操作

⑦　ユーザアカウントの作成、変更、追加　等

Ⅲ　個人情報の管理

学校における主な「個人情報※2」　※「写し」を含む

区分	書類・データ
学習指導に関するもの	□指導要録　□成績一覧表　□通知表 □個人名が特定される評価物（各種テストの答案を含む）
生徒指導に関するもの	□家庭環境調査票（家庭訪問は特例） □相談、面接、懇談記録　□事故報告書 □児童生徒理解のための会議資料　□特別指導に係る会議資料 □いじめ等調査に係る資料　□児童生徒指導計画　□特別支援会議記録 □特別支援教育に係る個別の教育支援計画、指導計画（家庭訪問、ケース会議は特例） □自立活動に関する記録、書類
進路指導に関するもの	□進路の合否に係るもの
健康・安全指導に関するもの	□健康診断票　□健康診断結果と統計　□保健に関する調査 □学校生活管理指導表　□児童生徒の傷病に係る診断書
その他	□出席簿　□会計簿　□児童生徒の異動に係るもの □就学支援金、就学奨励費に係るもの □教職員 G Suite for Education の ID・パスワード
その他、上記に準ずるもの	

1　個人が特定できる情報については、管理を徹底し、不特定多数が閲覧できる状況を作らないよう適切な場所や方法により保管すること。

2　個人が特定できる情報を、他人に利用させないこと。また共有しないこと。やむを得ず利用及び共有する場合は、教育情報セキュリティ管理者の承認を得ること。

3　個人が特定できる情報の照会には一切応じないこと。やむを得ない場合は、教育情報セキュリティ管理者の承認を得ること。

4　個人に配布した Google アカウントについては、各自責任をもって管理、保管すること。

5　個人が特定できる児童生徒の写真や動画については、校外に持ち出さないなど、取り扱いに十分配慮すること。なお個人情報の流失を防ぐため、私物のスマートフォンやデジタルカメラ等での撮影は極力避けること。

※２）個人情報

「個人情報とは，生存する個人に関する情報であって，当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別することができるものを含む。）をいう。

＜平成 16 年厚生労働省・経済産業省告示第４１号「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」より＞

Ⅳ　技術的セキュリティ

1　電子メールの扱いについて、以下を遵守すること

（1）教職員等は、自動転送機能を用いて電子メールを転送してはならない。

（2）教職員等は、業務上必要の無い送信先に電子メールを送信してはならない。

（3）教職員等は、重要な電子メールを誤送信した場合、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。

2　無許可ソフトウェア導入等の禁止

　教職員等は、パソコンやモバイル端末に、無断でソフトウェアを導入してはならない。業務上必要なソフトウェアを導入する場合は、事前に教育情報セキュリティ管理者と協議の上、美瑛町教育委員会の許可を得るものとする。

3　機器構成の変更の制限

　教職員等は、パソコンやモバイル端末に対し、機器の改造及び増設・交換を行ってはならない。

4　教職員等は、教育情報セキュリティ管理者の許可無く、パソコンやモバイル端末をネットワークに接続してはならない。

Ⅴ　情報セキュリティインシデント

1　教職員等は、情報セキュリティインシデントを認知した場合、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。

2　教職員等は、管理対象のネットワーク及び教育情報システム等の情報資産に関する情報セキュリティインシデントについて、外部から報告を受けた場合は、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。

3　不正プログラム対策として、教職員は以下の事項を遵守しなくてはならない。

（1）パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

（2）外部からデータ又は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わなければならない。

（3）差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

（4）端末に対して、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しなければならない。

（5）添付ファイルがついた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わなければならない。