日置市立湯田小学校　教育情報セキュリティポリシー

令和２年５月７日
日置市立湯田小学校

1　対象範囲及び用語説明

(1)　情報資産の範囲

本対策基準が対象とする情報資産は，次のとおりとする。

ア　教育ネットワーク，教育情報システム，これらに関する設備，電磁的記録媒体

イ　教育ネットワーク及び教育情報システムで取り扱う情報（これらを印刷した文書を含む。）

ウ　教育情報システムの仕様書及びネットワーク図等のシステム関連文書

(2)　用語説明

本対策基準における用語は，以下の通りとする。

用語	定義
校務系情報	児童の成績，出欠席及びその理由，健康診断結果，指導要録，教員の個人情報など，学校が保有する情報資産のうち，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	校務系情報のうち，保護者メールや学校ホームページ等インターネット接続を前提とした校務で利用される情報
学習系情報	児童のワークシート，作品など，学校が保有する情報資産のうち，それら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	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
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
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
学習系サーバ	学習系情報を取り扱うサーバ

2　組織体制

(1)　教育情報セキュリティ管理者

ア　校長を，**教育情報セキュリティ管理者**とする。

イ　教育情報セキュリティ管理者は当該学校の情報セキュリティ対策に関する権限及び責任を有する。

ウ　教育情報セキュリティ管理者は，当該学校において，情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には，市教育委員会へ速やかに報告を行い，指示を仰がなければならない。

3　情報資産の分類と管理方法

(1)　情報資産の分類

情報資産は，機密性，完全性及び可用性により，次のとおり分類し，必要に応じて取扱制限を行うものとする。

【機密性による情報資産の分類】

分類	分類基準	該当する情報資産のイメージ
機密性 3	学校で取り扱う情報資産のうち，秘密文書に相当する機密性を要する情報資産	特定の教職員のみが知り得る状態を確保する必要のある情報で秘密文書に相当するもの
機密性 2B	学校で取り扱う情報資産のうち，秘密文書に相当する機密性は要しないが，直ちに一般に公表することを前提としていない情報資産	教職員のみが知り得る状態を確保する必要がある情報資産（教職員のうち特定の教職員のみが知り得る状態を確保する必要があるものを含む）
機密性 2A	学校で取り扱う情報資産のうち，直ちに一般に公表することを前提としていないが，児童生徒がアクセスすることを想定している情報資産	教職員及び児童生徒同士のみが知り得る状態を確保する必要がある情報資産（教職員及び児童生徒のうち特定の教職員及び児童生徒のみが知り得る状態を確保する必要があるものを含む）
機密性 1	機密性 2A，機密性 2B 又は機密性 3 の情報資産以外の情報資産	公表されている情報資産又は公表することを前提として作成された情報資産（教職員及び児童生徒以外の者が知り得ても支障がないと認められるものを含む）

【完全性による情報資産の分類】

分類	分類基準	該当する情報のイメージ
完全性 2B	学校で取り扱う情報資産のうち，改ざん，誤びゅう又は破損により，学校関係者の権利が侵害される又は学校事務及び教育活動の的確な遂行に支障（軽微なものを除く）を及ぼすおそれがある情報資産	情報が正確・完全な状態である必要があり，破壊，改ざん，破損又は第三者による削除等の事故があった場合，業務の遂行に支障ある情報
完全性 2A	学校で取り扱う情報資産のうち，改ざん，誤びゅう又は破損により，学校関係者の権利が侵害される又は学校事務及び教育活動の的確な遂行に軽微な支障を及ぼすおそれがある情報資産	情報が正確・完全な状態である必要があり，破壊，改ざん，破損又は第三者による削除等の事故があった場合，業務の遂行に軽微な支障ある情報
完全性 1	完全性 2A 又は完全性 2B の情報資産以外の情報資産	事故があった場合でも業務の遂行に支障がない情報

【可用性による情報資産の分類】

分類	分類基準	該当する情報のイメージ
可用性 2B	学校で取り扱う情報資産のうち，滅失，紛失又は当該情報資産が利用不可能であることにより，学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	必要な時にいつでも利用できる必要があり，情報システムの障害等による滅失紛失や，情報システムの停止等があった場合，業務の安定的な遂行に支障がある情報
可用性 2A	学校で取り扱う情報資産のうち，滅失，紛失又は当該情報資産が利用不可能であることにより，学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に軽微な支障を及ぼすおそれがある情報資産	必要な時にいつでも利用できる必要があり，情報システムの障害等による滅失紛失や，情報システムの停止等があった場合，業務の安定的な遂行に軽微な支障がある情報
可用性 1	可用性 2A 又は可用性 2B の情報資産以外の情報資産	滅失，紛失や情報システムの停止等があっても業務の遂行に支障がない情報

(2)　情報資産の管理

ア　管理責任

(ｱ)　教育情報セキュリティ管理者は，その所管する情報資産について管理責任を有する。

(ｲ)　情報資産が複製又は伝送された場合には，複製等された情報資産も(1)の分類に基づき管理しなければならない。

イ　情報資産の分類の表示

教職員等は，情報資産について，ファイル（ファイル名，ファイルの属性（プロパティ），ヘッダー・フッター等），格納する電磁的記録媒体のラベル，文書の隅等に，情報資産の分類を表示し，必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

ウ　情報の作成

(ｱ)　教職員等は，業務上必要のない情報を作成してはならない。

(ｲ)　情報を作成する者は，情報の作成時に(1)の分類に基づき，当該情報の分類と取扱制限を定めなければならない。

(ｳ)　情報を作成する者は，作成途上の情報についても，紛失や流出等を防止しなければならない。また，情報の作成途上で不要になった場合は，当該情報を消去しなければならない。

エ　情報資産の入手

(ｱ)　学校内の者が作成した情報資産を入手した者は，入手元の情報資産の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者は，(1)の分類に基づき，当該情報の分類と取扱制限を定めなければならない。

(ｳ)　情報資産を入手した者は，その情報資産の分類が不明な場合，教育情報セキュリティ管理者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者は，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者は，情報資産の分類に応じ，適切な取扱いをしなければならない。

(ｳ)　情報資産を利用する者は，電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合，最高度の分類に従って，当該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)　教育情報セキュリティ管理者は，情報資産の分類に従って，情報資産を適切に保管しなければならない。

(ｲ)　教育情報セキュリティ管理者は，情報資産を記録した電磁的記録媒体を保管する場合は，書込禁止の措置を講じなければならない。

(ｳ)　教育情報セキュリティ管理者は，利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を保管する場合は，自然災害を被る可能性が低い地域に保管しなければならない。

(ｴ)　教育情報セキュリティ管理者は，機密性 2A 以上，完全性 2A 以上又は可用性 2A 以上の情報を記録した電磁的記録媒体を保管する場合，耐火，耐震，耐熱，耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

キ　情報の送信

電子メールにより機密性 2A 以上の情報を外部送信する者は，必要に応じ暗号化又はパスワード設定を行わなければならない。

ク　情報資産の運搬

(ｱ)　車両等により機密性 2A 以上の情報資産を運搬する者は，必要に応じ鍵付きのケース等に格納し，暗号化又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講じなければならない。

(ｲ)　機密性 2A 以上の情報資産を運搬する者は，教育情報セキュリティ管理者に許可を得なければならない。

ケ　情報資産の提供・公表

(ｱ)　機密性 2A 以上の情報資産を外部に提供する者は，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。

(ｲ)　機密性 2A 以上の情報資産を外部に提供する者は，教育情報セキュリティ管理者に許可を得なければならない。

(ｳ)　教育情報セキュリティ管理者は，住民に公開する情報資産について，完全性を確保しなければならない。

コ　情報資産の廃棄

(ｱ)　機密性 2A 以上の情報資産を廃棄する者は，情報を記録している電磁的記録媒体が不要になった場合，電磁的記録媒体の初期化等，情報を復元できないように処置した上で廃棄しなければならない。

(ｲ)　情報資産の廃棄を行う者は，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)　情報資産の廃棄を行う者は，教育情報セキュリティ管理者の許可を得なければならない。

4　物理的セキュリティ

(1)　管理区域の管理

ア　管理区域の入退室管理等

(ｱ)　教職員は，児童生徒が管理区域に入室する場合，必要に応じて立ち入り区域を制限した上で，児童生徒に付き添うものとする。

(ｲ)　外部委託事業者は，管理区域に入室する場合，身分証明書等を携帯し，求めにより提示しなければならない。

(ｳ)　教育情報システム管理者は，外部からの訪問者が管理区域に入る場合には，必要に応じて立ち入り区域を制限した上で，管理区域への入退室を許可された教職員等が付き添うものとし，外見上教職員等と区別できる措置を講じなければならない。

イ　機器等の搬入出

教育情報システム管理者は，情報システム室の機器等の搬入出について，教職員を立ち会わせなければならない。

(2)　教職員等の利用する端末や電磁的記録媒体等の管理

ア　校務用端末，校務外部接続用端末及び指導者用端末について

(ｱ)　盗難防止のため，職員室等で利用する校務用端末及び校務外部接続用端末のワイヤーによる固定，教室等で使用する指導者用端末の保管庫による管理等，使用する目的に応じた適切な物理的措置を講じなければならない。電磁的記録媒体については，情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

(ｲ)　情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

(ｳ)　端末の電源起動時のパスワード（BIOS パスワード，ハードディスクパスワード等）を設定しなければならない。

(ｴ)　取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の二要素認証を設定しなければならない。

(ｵ)　パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合，その機能を有効に活用しなければならない。同様に，電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。

(ｶ)　モバイル端末の学校外での業務利用の際は，上記対策に加え，遠隔消去機能を利用する等の措置を講じなければならない。

イ　学習者用端末について

(ｱ)　盗難防止のため，教室等で利用するパソコンの保管庫による管理等の物理的措置を講じなければならない。電磁的記録媒体については，情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

(ｲ)　情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

5　人的セキュリティ

(1)　教職員等の遵守事項

ア　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資産の外部への持ち出し，教育情報システムへのアクセス，電子メールアドレス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)　モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

a　教職員等は，学校のモバイル端末，電磁的記録媒体，情報資産及びソフトウェアを外部に持ち出す場合には，教育情報セキュリティ管理者の許可を得なければならない。

b　教職員等は，外部で情報処理業務を行う場合には，教育情報セキュリティ管理者の許可を得なければならない。

(ｳ)　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の業務利用

a　教職員等は，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原則業務に利用してはならない。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利用することができる。

b　教職員等は，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用いる場合には，教育情報セキュリティ管理者の許可を得た上で，外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

(ｴ)　持ち出し及び持ち込みの記録

教育情報セキュリティ管理者は，端末等の持ち出し及び持ち込みについて，記録を作成し，保管しなければならない。

(ｵ)　パソコンやモバイル端末におけるセキュリティ設定変更の禁止

教職員等は，パソコンやモバイル端末の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セキュリティ管理者の許可なく変更してはならない。

(ｶ)　机上の端末等の管理

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。

(ｷ)　退職時等の遵守事項

教職員等は，異動，退職等により業務を離れる場合には，利用していた情報資産を，返却しなければならない。また，その後も業務上知り得た情報を漏らしてはならない。

イ　情報セキュリティポリシー等の掲示

教育情報セキュリティ管理者は，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できるように掲示しなければならない。

(2)　研修・訓練

ア　研修計画の策定及び実施

(ｱ)　研修計画において，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できるようにしなければならない

イ　研修・訓練への参加

全ての教職員等は，定められた研修・訓練に参加しなければならない。

(3)　情報セキュリティインシデントの報告

ア　学校内からの情報セキュリティインシデントの報告

(ｱ)　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。

(ｲ)　報告を受けた教育情報セキュリティ管理者は，速やかに市教育委員会に報告しなければならない。

イ　住民等外部からの情報セキュリティインシデントの報告

(ｱ)　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，住民等外部から報告を受けた場合，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。

(ｲ)　報告を受けた教育情報セキュリティ管理者は，市教育委員会に報告しなければならない。

(4)　ID及びパスワードの管理

ア　IDの取扱い

教職員等は，自己の管理するIDに関し，次の事項を遵守しなければならない。

(ｱ)　自己が利用しているIDは，他人に利用させてはならない。

(ｲ)　共用IDを利用する場合は，共用IDの利用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，次の事項を遵守しなければならない。

(ｱ)　パスワードは，他者に知られないように管理しなければならない。

(ｲ)　パスワードを秘密にし，パスワードの照会等には一切応じてはならない。

(ｳ)　パスワードは十分な長さとし，文字列は想像しにくいものにしなければならない。

(ｴ)　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。

(ｵ)　パスワードは定期的に又はアクセス回数に基づいて変更し，古いパスワードを再利用してはならない。

ウ　複数の教育情報システムを扱う教職員等は，同一のパスワードを複数のシステム間で用いてはならない。

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てはならない。

カ　教職員等間でパスワードを共有してはならない。

6　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)　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。

(ｲ)　教職員等は，業務上必要のない送信先に電子メールを送信してはならない。

(ｳ)　教職員等は，複数人に電子メールを送信する場合，必要がある場合を除き，他の送信先の電子メールアドレスが分からないようにしなければならない。

(ｴ)　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。

(ｵ)　教職員等は，ウェブで利用できるフリーメールサービス等許可無しに使用してはならない。

イ　電子署名・暗号化

(ｱ)　教職員等は，情報資産の分類により定めた取扱制限に従い，外部に送るデータの機密性又は完全性を確保することが必要な場合には，市教育委員会が定めた電子署名，暗号化又はパスワード設定等，セキュリティを考慮して，送信しなければならない。

(ｲ)　教職員等は，暗号化を行う場合に市教委が定める以外の方法を用いてはならない。また，市教委が定めた方法で暗号のための鍵を管理しなければならない。

ウ　無許可ソフトウェアの導入等の禁止

(ｱ)　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。

(ｲ)　教職員等は，業務上の必要がある場合は，市教育委員会の許可を得て，ソフトウェアを導入することができる。なお，導入する際は，教育情報セキュリティ管理者は，ソフトウェアのライセンスを管理しなければならない。

(ｳ)　教職員等は，不正にコピーしたソフトウェアを利用してはならない。

エ　機器構成の変更の制限

(ｱ)　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。

(ｲ)　教職員等は，業務上，パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には，統括教育情報セキュリティ責任者及び教育情報システム管理者の許可を得なければならない。

オ　無許可でのネットワーク接続の禁止

教職員等は，統括教育情報セキュリティ責任者の許可な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。

カ　業務以外の目的でのウェブ閲覧の禁止

教職員等は，業務以外の目的でウェブを閲覧してはならない。

(2)　アクセス制御

ア　アクセス制御等

(ｱ)　教職員等は，業務上必要がなくなった場合は，利用者登録を抹消するよう，教育情報セキュリティ管理者を通して，市教育委員会に通知しなければならない。

イ　教職員等による外部からのアクセス等の制限

(ｱ)　教職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は，市教育委員会の許可を得なければならない。

(ｲ)　教職員等は，持ち込んだ又は外部から持ち帰ったモバイル端末を施設内のネットワークに接続する前に，コンピュータウイルスに感染していないこと，パッチの適用状況等を確認しなければならない。

(3)　不正プログラム対策

ア　教職員等の遵守事項

教職員等は，不正プログラム対策に関し，次の事項を遵守しなければならない。

(ｱ)　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。

(ｲ)　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。

(ｳ)　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。

(ｴ)　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。

(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わなければならない。

(ｶ)　市教育委員会が提供するウイルス情報を，常に確認しなければならない。

(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，以下の対応を行わなければならない。

a　パソコン等の端末の場合

LAN ケーブルの即時取り外しを行わなければならない。

b　モバイル端末の場合

直ちに利用を中止し，通信を行わない設定への変更を行わなければならない。

7　運用

(1)　情報セキュリティポリシーの遵守状況の確認

ア　遵守状況の確認及び対処

(ｱ)　教育情報セキュリティ管理者は，教育情報セキュリティポリシーの遵守状況について確認を行い，問題を認めた場合には，速やかに市教育委員会に報告しなければならない。

イ　教職員等の報告義務

(ｱ)　教職員等は，教育情報セキュリティポリシー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に報告を行わなければならない。

(ｲ)　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると判断した場合は，緊急時対応計画に従って適切に対処しなければならない。

(2)　法令等遵守

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 12 月 13 日法律第 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 5 月 30 日法律第 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　個人情報保護条例

(3)　懲戒処分等

ア　懲戒処分

教育情報セキュリティポリシーに違反した教職員等及びその監督責任者は，その重大性，発生した事案の状況等に応じて，地方公務員法による懲戒処分の対象とする。

8　外部サービスの利用

(1)　ソーシャルメディアサービスの利用

ア　教育情報システム管理者は，教育委員会又は学校が管理するアカウントでソーシャルメディアサービスを利用する場合，情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(ｱ)　本市のアカウントによる情報発信が,実際の本市のものであることを明らかにするために，本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに，当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

(ｲ)　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適切に管理するなどの方法で，不正アクセス対策を行うこと

イ　機密性 2A 以上の情報はソーシャルメディアサービスで発信してはならない。

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。

9　評価・見直し

(1)　自己点検

ア　実施方法

(ｱ)　教育情報セキュリティ管理者は,教育情報セキュリティポリシーに沿った情報セキュリティ対策状況について，毎年度及び必要に応じて自己点検を行わなければならない。

イ　自己点検結果の活用

(ｱ)　教職員等は，自己点検の結果に基づき，自己の権限の範囲内で改善を図らなければならない。

(ｲ)　情報セキュリティ委員会は,この点検結果を情報セキュリティポリシー及び関係規程等の見直し，その他情報セキュリティ対策の見直し時に活用しなければならない。

(2)　教育情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は，情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ，情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い，必要があると認めた場合，改善を行うものとする。

日置市立湯田小学校ホームページ作成上のガイドライン

日置市立湯田小学校情報管理委員会
平成１９年４月１８日　作成
平成３０年３月２３日　改訂

１　目的

(1)　学校広報としての役割をもった情報発信をする。

ア　学校要覧として公開されてきたものを基本とし，大体の学校情報と連絡手段を明示するようにする。

イ　本校の教育活動についての理解を促すために，学校の実践・創造的活動内容を公開する。

(2)　学習の一環として，情報発信をする。

ア　学習のまとめを発信することで，情報社会に参画する態度を養う。

２　作成内容について

ホームページ作成については，特に，児童のプライバシーの保護，人権への配慮，知的所有権（著作権や肖像権など）の遵守の３点に気をつけて作成する。

(1)　公開しないもの

ア　児童写真から個人名が特定できるもので保護者の承諾がないもの。
（一人で写り，名前と顔写真が一致するもの。）

イ　個人生活に関する情報
実名，国籍，本籍，住所，電話番号，生年月日，家族構成など

ウ　著作権のあるもの
アニメや漫画などのキャラクターの似顔絵，本や新聞の記事や写真等

エ　他人の誹謗・中傷や差別につながるようなこと

オ　その他，学校長又は情報管理委員会が，学校から不特定多数に対して発信する情報として不適当と判断する内容（営利目的，法令及び公序良俗違反など）

(2)　条件付きで公開するもの

ア　児童写真
第三者が閲覧して，個人名が特定できないものにする。
２名以上の児童，保護者がうつっているものや全体を捉えたものにする。

イ　児童の作品（絵画や工作など）
教育上効果があると認められた上で，本人の承諾を得る。

ウ　個人名が特定される
児童１名だけがうつっており，名前も掲載されている。保護者の承諾を得る。

エ　新聞記事，写真など著作権のあるもの
著作権者に承諾を得る。

オ　児童名
ただし，本人及び保護者からの承諾がとれたもの，学校だより等ですでに公開されているものは除く。

３　作成内容について

(1)　作成ページに関しては，原則として，校長決裁をうけることとする。

(2)　新規ページは，各カテゴリー内に新規フォルダを作成し，構成するファイルをそのフォルダ内に全て転送し，管理運営にあたることとする。

4　ホームページ公開までの手順と公開後の管理について

(1)　公開するデータのチェック機関は，情報管理委員会とする。

(2)　公開までの手順

ア　情報発信者は「ホームページ作成のためのガイドライン」をもとにデータを作成し，情報管理委員会に提出する。

イ　情報管理委員会のチェックを受けたデータは，取扱責任者が集約し，管理責任者に提出する。管理責任者は，学校長の決済を受ける。

ウ　学校長の決済を受けたデータは，取扱責任者がサーバーにアップする。

エ　すでに公開されているデータが更新された場合も，上記手順をふむ。

(3)　公開後の管理について

ア　公開されたデータは，全職員で日常的にチェックする。

イ　問題が発生した場合は，情報管理委員会で協議する。委員会で対処できない場合は校内で協議するが，いずれにしても最終的には学校長が判断する。

4　責任範囲について

(1)　責任者について

学校ホームページに掲載された情報について，学校長は責任を負う。

(2)　取扱責任者について

学校長は，インターネット利用及びホームページ作成の適正を図るために，校内の情報教育係及び情報管理委員会から管理責任者及び取扱責任者をおくものとする。

情報管理委員会は，作成された Web ページが本ガイドラインにそったものであるか検討する。検討された Web ページは，管理責任者を通し，校長の決済をうけた上で，取扱責任者がアップする。

(3)　教職員及び保護者，地域住民等が校内で授業参観，学校行事等を撮影した情報を，学校の決済なく，ＳＮＳ等で公開した画像，文書等については，学校は責任を負わない。

また，上記については，学校として啓発を行い周知を図る。

5　その他

(1)　掲載情報に対する指摘への対応

児童に関する掲載情報について，本人又は保護者から掲載内容の訂正や削除の要請を受けた場合には，速やかに要請に対応した措置を講じる。第三者の著作に係る情報について当該著作権者から要請があった場合も同様とする。その他，閲覧者等から掲 載情報の内容について指摘を受けた場合には，速やかに情報管理委員会で協議した後，適切な措置を講じることとする。

(2)　本ガイドラインの見直し

ネット社会における情報モラルの考え方の進展に伴い，このガイドラインに示した事項の見直しが予想されるため，ガイドラインの定期的な検討と，加筆・修正を行うものとする。