# 石岡市教育情報
# セキュリティポリシー

＜教育情報セキュリティ基本方針＞

石岡市教育委員会

令和８年３月版

＜　目　　次　＞



石岡市教育情報セキュリティポリシー改正履歴

令和８年３月　　策定

## １　目的と位置付け

小・中学校が取り扱う情報には、児童・生徒の個人情報のみならず保護者、教職員、その他地域住民に関する情報等、学校運営に欠かせない重要な情報が数多く含まれており、外部への情報漏えい等が発生した場合には、極めて重大な結果を招くおそれがある。

したがって、本市の教育情報に係る各種ネットワークにおいて、個人情報を始めとする情報資産を漏えいや改ざん、コンピュータウイルスによるシステム障害、災害や事故等の様々な脅威から防御することは、保護者や地域住民等から信頼される安心・安全な学校づくりには必要不可欠なことである。

また、ＧＩＧＡスクール構想における１人１台端末の整備に伴い、学校内外において、児童・生徒が安全にＩＣＴを活用するための環境を整備する責務がある。

こうしたことから、市立小・中学校における情報セキュリティ対策を総合的、体系的かつ具体的に整備することを目的に、教育情報セキュリティポリシーを定めることとする。

## ２　教育情報セキュリティポリシーの位置付け

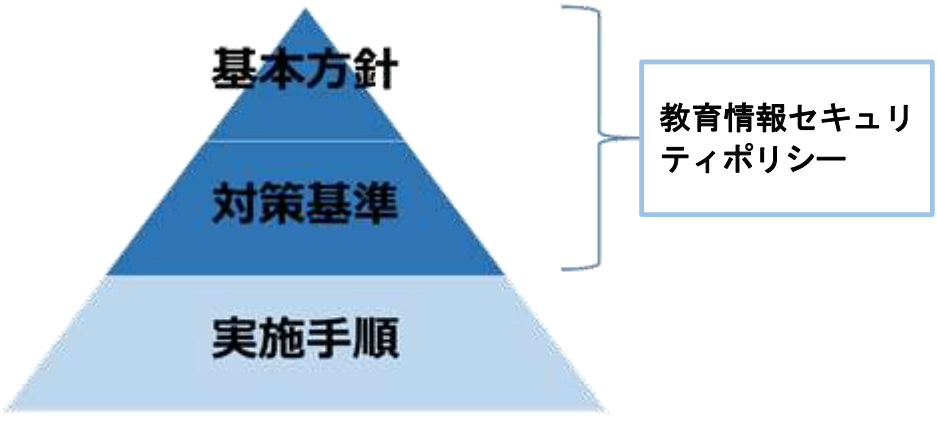
教育情報セキュリティポリシーは「教育情報セキュリティ基本方針」、「教育情報セキュリティ対策基準」の２つから構成される。（下図参照）また、教育情報セキュリティポリシーに基づき、教育情報システム毎の具体的な情報セキュリティ対策の実施手順として「教育情報セキュリティ実施手順書」を策定する。

（１）　教育情報セキュリティ基本方針
　　教育情報セキュリティ対策に関する統一的かつ基本的な方針。

（２）　教育情報セキュリティ対策基準
　　教育情報セキュリティ基本方針を実行に移すためのすべてのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。

（３）　教育情報セキュリティ実施手順書
　　ネットワーク及び情報システム毎に定める教育情報セキュリティ対策基準に基づいた具体的な実施手順。

なお、教育情報セキュリティ対策基準及び教育情報セキュリティ実施手順書については、公にすることにより行政運営に重大な支障を及ぼす情報であることから非公開とする。



## 3　定義

（1）　教育情報システム

本市の学校教育において使用されるサーバ及び端末（ネットワーク、ハードウェア及びソフトウェア）並びに記録媒体等で構成され、処理を行う仕組みをいう。

（2）　情報資産

対象とする情報資産は、次のとおりとする。

ア　教育情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　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関連文書

（3）　情報セキュリティ

情報資産の機密の保持並びに正確性及びの維持並びに定められた範囲での利用可能な状態を維持することをいう。

（4）　教職員

学校教育法（昭和 22 年法律第 26 号）第 37 条及び第 49 条に規定する者で、市長が設置する小・中学校に従事する職員並びにその他の支援員等をいう。

（5）　児童

学校教育法（昭和 22 年法律第 26 号）第 17 条第 1 項及び第 18 条に規定する者で、市長が設置する小学校に在学するものをいう。

（6）　生徒

学校教育法（昭和 22 年法律第 26 号）第 17 条第 1 項及び第 18 条に規定する者で、市長が設置する中学校に在学するものをいう。

## 4　教育情報セキュリティポリシーの位置づけと教職員等の責務

教育情報セキュリティポリシーは、本市が所管する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、教育情報セキュリティ対策の頂点に位置するものである。

したがって、本市の教職員、情報資産に係る業務に携わる教育委員会事務局の職員（会計年度任用職員及び再任用職員等を含む)、外部委託事業者に属する者（以下「教職員等」という。）は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たって、教育情報セキュリティポリシーを遵守する義務を負うものとする。

## 5　教育情報セキュリティ管理体制

本市の情報資産について、情報セキュリティ対策を推進し、管理するための体制を確立するものとする。

## 6　情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

## 7　情報資産への脅威

教育情報セキュリティポリシーを策定する上で、情報資産に対する脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は、次のとおりである。

（1） 部外者の侵入、盗難及び故意の不正アクセス又は不正操作による機器若しくは情報資産の破壊、漏えい・改ざん・消去、重要情報の搾取、内部不正等盗聴等

（2） 教職員等による機器若しくは情報資産の持出し又は誤操作及びアクセスのための認証情報若しくはパスワードの不適切管理、無許可ソフトウェアの使用、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、機器故障等の非意図的要因、故意の不正アクセス若しくは不正行為による破壊、盗聴、改ざん、消去等、搬送中の事故等による機器又は情報資産の盗難並びに規定外の端末接続によるデータ漏えい等

（3） コンピュータウイルス、地震、落雷、火災等の災害、事故、故障等によるサービス及び業務の停止

（4） 大規模・広範囲にわたる疫病による要員不足に伴うシステム運用の機能不全等

（5） 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

## 8　教育情報セキュリティ対策

7で示した脅威から情報資産を保護するために、次の情報セキュリティ対策を講ずるものとする。

（1） 物理的セキュリティ対策
教育情報システムを設置する施設への不正な立入り、情報資産への損傷及び妨害等から保護するための物理的な対策

（2） 人的セキュリティ対策
情報セキュリティに関する権限や責任を定め、教職員等に教育情報セキュリティポリシーの内容を周知徹底するための十分な教育及び啓発

（3） 技術的セキュリティ対策
情報資産を外部からの不正なアクセス等から適切に保護するための情報資産へのアクセス制御、ネットワーク管理等の技術面の対策

（4） 運用
教育情報システムの監視、教育情報セキュリティポリシーの遵守状況の確認等の運用面の対策及び緊急事態が発生した際に迅速な対応を可能とするための危機管理対策

（5） 外部委託
外部委託事業者からの情報漏えい等の事案を防止し、情報セキュリティを確保するための措置として、外部委託事業者の選定基準、契約項目等を定める。

（6） クラウドサービスの利用

クラウドサービスの利用に当たり、サービス提供事業者に要求するセキュリティ対策の項目等を定める。約款による外部サービスの利用及びソーシャルメディアサービスの利用基準等は別に定める。

（7）　１人１台端末におけるセキュリティ
不適切なウェブページの閲覧防止等、児童・生徒が安全に端末を利用するための、１人１台端末に対するセキュリティ対策

## 9　教育情報セキュリティ対策基準の策定

本市の様々な情報資産について、８の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。このため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した教育情報セキュリティ対策基準を策定する。

## 10　教育情報セキュリティ実施手順の策定

教育情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、情報資産ごとに実施手順等をそれぞれ定めていく必要がある。このため、情報資産に対する脅威及び情報資産の重要度に対応する教育情報セキュリティ対策基準の基本的な要件に基づき、情報資産の情報セキュリティ実施手順を策定するものとする。

なお、教育情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがある情報資産であることから非公開とする。

## 11　教育情報セキュリティ監査の実施

教育情報セキュリティポリシーが遵守されていることを検証するため、定期的及び必要に応じて監査を実施する。

## 12　評価及び見直しの実施

教育情報セキュリティ監査の結果等により、教育情報セキュリティポリシー及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するため、教育情報セキュリティポリシーの見直しを実施する。