

厚木市教育情報セキュリティポリシー

【公開版】

この文書は、厚木市教育委員会及び厚木市立小・中学校外に非公開としている「教育情報セキュリティ対策基準」を含みません。

平成31年3月1日	策定
令和2年11月17日	改定
令和3年4月1日	改定
令和5年11月1日	改定
令和7年12月1日	改定

厚木市教育委員会

<目 次>

第1章 教育情報セキュリティ基本方針

1	目的	1
2	定義	1
	(1) 教育情報システム	1
	(2) 情報資産	1
	(3) 情報セキュリティ	1
	(4) 教職員	1
	(5) 児童	1
	(6) 生徒	1
3	教育情報セキュリティポリシーの位置付けと教職員等の義務	2
4	教育情報セキュリティ管理体制	2
5	情報資産の分類	2
6	情報資産への脅威	2
7	教育情報セキュリティ対策	2
	(1) 物理的セキュリティ対策	2
	(2) 人的セキュリティ対策	2
	(3) 技術的セキュリティ対策	2
	(4) 運用	3
	(5) 外部委託	3
	(6) クラウドサービスの利用	3
	(7) 1人1台端末におけるセキュリティ	3
8	教育情報セキュリティ対策基準の策定	3
9	教育情報セキュリティ実施手順の策定	3
10	教育情報セキュリティ監査の実施	3
11	評価及び見直しの実施	3

第1章 教育情報セキュリティ基本方針

1 目的

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等が数多く含まれ、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、マルウェア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。

このうち基本方針は、各小・中学校が所管する情報資産においても、本市全体の基本方針と共通のものであるとの認識の上に立ち、厚木市情報セキュリティ基本方針を準用するものとする。

2 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 教育情報ネットワーク及び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教育情報ネットワーク図等のシステム関連文書

(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完全性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2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。

3 教育情報セキュリティポリシーの位置付けと教職員等の義務

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、指定管理者及び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。

4 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。

5 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。

6 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、盗聴、改ざん、消去等
- (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、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) マルウェア、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

7 教育情報セキュリティ対策

6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

不適切なウェブサイトの閲覧防止等、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

8 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、7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。

なお、教育情報セキュリティ対策基準は、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。

9 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。

10 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。

11 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。