

教育情報セキュリティに関する学校ガイドライン

令和5年4月1日

座間市立東中学校教育情報セキュリティ委員会

—目 次—

1	趣旨	p 2
2	目的	p 2
3	校内教育情報セキュリティ委員会	p 2
4	機器等の運用・管理	p 3
5	ソフトウェアの運用・管理	p 3
6	PC教室の利用	p 4
7	タブレット型PCの利用	p 4
8	教職員のネットワークによる情報発信	p 5
9	児童・生徒のネットワーク（インターネット等）の利用	p 5
10	学校ホームページ	p 5
11	電子メール等の利用	p 6
12	守秘義務	p 6
13	個人情報保存・管理	p 6
14	トラブルの対策	p 8
15	本ガイドラインの見直し及び指導	p 9
16	違反者への対応	p 9
17	その他	p 9

(趣旨)

- 1 このガイドラインは、「座間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」および「教育情報セキュリティ対策基準」）に基づき座間市立東中学校の教育情報セキュリティに関して必要な事項を定めるものとする。
なお、本ガイドラインは「教育情報セキュリティ基本方針」第10項に定める「教育情報セキュリティ実施手順」にあたり、公開することで運営に重大な支障を及ぼす恐れがあることから、非公開とする。

(目的)

- 2 教育情報セキュリティに関して、児童・生徒及び関係者の個人情報の保護に努めるとともに、児童・生徒の発達段階に応じた情報活用能力と情報モラルの育成を図り、校務での活用を進め、教育活動をより充実し推進するために行うものとする。

(校内教育情報セキュリティ委員会)

- 3 「教育情報セキュリティ対策基準」第2項により、校内の教育情報セキュリティ対策の適正を図るために「校内教育情報セキュリティ委員会」を設置する。

(1) 組織

※校長・教頭・情報教育推進担当教員の役職名は「教育情報セキュリティ対策基準」に則る。なお、これ以降の表記は校長・教頭・情報教育推進担当者とする。

ア 教育情報セキュリティ管理者（校長）

イ 教育情報セキュリティ担当者（教頭）

※校長が指名した者で原則は教頭が務める。ウと兼務は不可とする。

ウ 委員長（リーダー） 1名（大岩）

※校務分掌上では情報教育推進担当者（主の者）とする。

エ 副委員長 1名（佐藤）

オ 委員 若干名（総括教諭・情報担当（藤井、山戸、神崎、池上））

(2) 役割

ア 「教育情報セキュリティ対策基準」の適正な運用

イ 教育情報セキュリティに関する学校ガイドラインの作成と周知

ウ 教育情報セキュリティに関する運用・管理

- ・ PC教室利用の運用・管理（利用割り当て・利用記録簿の運用等）
- ・ 教育用PC（教師の授業用および学習者用PC）の運用・管理
- ・ 校務用PC（成績処理や保健事務などの校務用PC）の運用・管理
- ・ 校内サーバおよび公的USB等の運用・管理

- ・周辺 I C T 機器の運用・管理
- エ 教育の情報化推進
 - ・機器操作、モラル教育、教育情報セキュリティなどの各種研修の計画・実施
- オ ネットワーク利用等のトラブルへの対応
 - ・機器に関するトラブル発生時の対応
 - ・情報管理に関するトラブル発生時の対応
 - ・その他
- カ ネットワーク機器の管理
 - ・教育コンテンツ、ソフトウェアの管理、電子データの保管ルールの周知・ウィルス定義ファイルの更新
 - ・データの管理
 - ・その他
- キ 学校ホームページ
 - ・企画、構成、作成計画、著作権・肖像権の許諾等
 - ・情報掲載の承諾、学校ホームページの更新
- ク 自己点検
 - ・認められていない活動を検知するため、および学校ガイドラインの実行性を維持するために必要な対策の一環として、校長の責任の下、必要に応じて自己点検を行う。
- ケ その他
 - ・校内の実態把握

(機器等の運用・管理)

- 4 機器等の運用・管理については「教育情報セキュリティ対策基準」及び次の点に留意する。
- (1) 校内ネットワークに接続できるコンピュータ等は、教育委員会が指定したものとする。
 - (2) 補助記憶装置の使用については、「教育情報セキュリティ対策基準」に則ることとする。
 - (3) コンピュータ等の情報機器については、原則、持ち出し禁止とする。やむを得ず校外へ持ち出す場合においては、教頭を通して校長の許可を得る。また、持ち出しの事実について記録しなければならない。
 - (4) コンピュータは、鍵のかかる保管場所または、盗難防止ワイヤー等で管理をする。

(ソフトウェアの運用・管理)

- 5 ソフトウェアの運用・管理については「教育情報セキュリティ対策基準」及び次の点に留意する。
- (1) 共通に導入されているソフトウェア以外のもので利用を希望する際には校内教育情報セキュリティ委員会で検討し、教育委員会に所定の様式で届け出て承認を受けるものとする。
 - (2) ライセンスの管理に関しては情報教育推進担当者が適正に管理する。

(PC教室の利用)

- 6 PC教室の利用については「教育情報セキュリティ対策基準」及び次の点に留意する。
- (1) 使用については学習活動での利用を原則とする。使用については、利用割り当てに従い、事前に利用予定表に記入し、使用の際には必ず利用記録簿に記入をする。この際、複数の授業で同じ時間帯に利用希望があったときには指導者同士で協議する。
 - (2) 使用後は使用教師の責任においてコンピュータ及びサーバに不要なデータを残さない。
 - (3) 年度末にはデータ整理の確認をし、必要に応じて名簿の更新等を行なう。
 - (4) 休み時間などに、児童・生徒がPC教室を使用する場合、教師が必ず付き添うこととする。学習に関係のない使用は禁止とする。

(タブレット型PCの利用)

- 7 タブレット型PCの利用については「教育情報セキュリティ対策基準」及び次の点に留意する。
- (1) タブレット型PCの管理は、教育委員会の指示の下、学校で管理する。
 - (2) 故障の際の代替機運用については、教育委員会の指示の下、学校で対応する。
 - (3) 充電は学校及び家庭で行う。学校での充電方法は教育委員会の指示の下、校内教育情報セキュリティ委員会で協議の上、ルールに則り行う。
 - (4) 教職員が授業や教材研究等でタブレット型PCを使用する方法については教育委員会の指示の下、校内教育情報セキュリティ委員会で協議の上、ルールに則り行う。
 - (5) 児童・生徒の使用については、学習活動での利用とする。放課後など授業への支障がない場合に限り、教師が校務で使用することは可能とするが、データを端末内に残してはならない。
 - (6) 休み時間などに、児童・生徒がタブレット型PCを使用する際は、担当教師の指導の下行うこととする。学習に関係のない使用は禁止とする。

- (7) 教科指導及び学習に必要なデータのクラウド保存については、「教育情報セキュリティ対策基準」及び「クラウドサービス利用実施手順」に則ること。
- (8) 端末本体にデータは保存しないこと。

(教職員のネットワークによる情報発信)

- 8 ネットワークを通じて情報を発信する場合は、「教育情報セキュリティ対策基準」また「クラウドサービス利用実施手順」及び次の点に留意する。
 - (1) ネットワークを利用して児童の個人情報を外部へ発信する場合には、本人及び保護者の同意を前提とする。児童・生徒が発信する場合は、教師の指導のもとに発信するものとする。また、ネットワークで発信する児童・生徒の個人情報の範囲は次のように定める。
 - ア 児童の作品及び学習成果等においては、原則として姓名は使わないが、作品が入賞・入選する等、教育上必要がある場合には、本人及び保護者の同意のもとに姓名を使うことも可とする。
 - イ 意見・主張等児童の意見、考え等については個人情報の内容と教育上の効果を斟酌し発信することができる。
 - ウ 写真等個人が特定できないように配慮する。

(児童・生徒のネットワーク（インターネット等）の利用)

- 9 児童がネットワークを利用する場合は、「教育情報セキュリティ対策基準」また「クラウドサービス利用実施手順」及び次の点に留意する。
 - (1) 学校において児童がネットワークを利用する場合は、必ず教師の指導のもとで行う。
 - (2) 学校において児童が外部にデータを発信する場合、必ず教師の指導のもとで内容の検討及び確認を行い、校長の許可を得ることとする。
 - (3) 教師は予め検索すべき課題内容の検討及び確認を行いネットワーク利用における安全の確保に努める。
 - (4) 教育上有害と認められる情報は閲覧を禁止することとする。
 - (5) インターネットの立ち上げ時は、適切なページに設定しておく。
 - (6) 「お気に入り」への追加は、学習に必要なページのみとし、必要がなくなり次第、削除すること。また、履歴は随時削除すること。

(学校ホームページ)

- 10 学校ホームページを利用し、ネットワークを通じて情報を発信する場合は「教育情報セキュリティ対策基準」及び次の点に留意する。
 - (1) 学校ホームページに掲載する内容は校内教育情報セキュリティ委員会で検討

し、校長の承認を得て情報発信を行う。

- (2) 学校ホームページの企画、構成、作成計画、著作権・肖像権の許諾等については、校内教育情報セキュリティ委員会が検討し、問題がないことを確認する。
- (3) 著作物を学校ホームページで発信する場合は著作者の許諾を得ることとし、児童が作成した作品や児童の個人が特定できる写真は本人及び保護者の同意を得ることとする。

(電子メール等の利用)

- 11 電子メールの利用について、ネットワークを通じて情報を発信する場合は、「情報セキュリティ対策基準」及び次の点に留意する。
 - (1) 公序良俗に反しないこと。
 - (2) 犯罪行為に結びつけないこと。
 - (3) 法令に違反しないこと。
 - (4) 他に不利益を与えないこと。
 - (5) 他を誹謗中傷しないこと。
 - (6) 宛先を間違えないよう注意すること。
 - (7) 相手を意識したマナー・エチケットに心がけること。
 - (8) 児童・生徒が学校外へメールを発信する際は、個人情報が含まれる場合は本人と保護者の同意を前提とし、教員の指導のもとに行なわれること。
 - (9) 学校メールは、1日1回は受信、内容確認を行うこと。
 - (10) 校長・教頭・学校代表・その他役職等に配付されているメールアカウントを変更することを禁ずる。なお、児童・生徒及び教職員のWEBメールアカウントの管理については、「クラウドサービス利用実施手順」に則る。
 - (11) 学校間のメールでの問合せなど、学校のメールアドレスで届いたものは文書と同じ扱いで担当者が校長の判断を得て返信する。また、個人に届いたものでも、学校書類として送られてきたものは校長の判断を得て返信する。
 - (12) 一斉メール配信システムおよび学習支援システムのメール機能の利用については校内教育情報セキュリティ委員会および校長の許可の下、適切に運用する。原則、校務外のことについて、児童・生徒および保護者と個人的な連絡のやりとりをすることは厳に禁ずる。

(守秘義務)

- 12 教職員は地方公務員法第34条に規定する守秘義務を遵守するとともに、学校で得た個人に関する情報をみだりに発信し、または受信してはならない。

(個人情報保存・管理)

13 個人情報保存・管理については、「教育情報セキュリティ対策基準」及び次の点に留意する。

- (1) 成績処理や個人情報処理等を行なう際は、認証キー等を利用し、ネットワークから遮断すること。
- (2) 個人情報を含む文書の電子データは、持ち出し禁止とする。
- (3) 個人情報を含む文書の電子データは、校内教育情報セキュリティ委員会が定めるルールに則り管理する。校務用・教育用問わずあらゆる端末に保存することを禁ずる。また、校内サーバ及び公的USBに長期間保存されたままになることがないように、年度内に1回以上の点検・整理を行なう。必要に応じて保存すべきデータはDVD等に移し、校内教育情報セキュリティ委員会の責任下で適切に保管する。
- (4) 校長は異動する教職員に、使用した電子データの消去を指示し、実施の報告を受けて確認をする。
- (5) 個人が特定できる個人情報を含む画像、動画、音声の電子データは、原則、持ち出し禁止とする。
- (6) 個人情報を含む電子データの秘密を保持するとともに、漏えい・紛失・き損等の防止の意識を高める。
- (7) 個人情報を含む電子データを部外者へ提供してはならない。ただし、当該データに関する権利を有する者が認め、校長が承認するときはこの限りではない。
- (8) 公的USBメモリーの運用については、「教育情報セキュリティ対策基準」に基づく。なお、公的USBメモリーの使用はデータの移動等、必要最小限に留め、校外への持ち出しは原則禁止とする。

(その他公的USB関連事項)

- ・学校で一括管理し、個人で管理しない。管理台帳で数量の把握を行う。
- ・成績処理等やむを得ず公的USBメモリーを校外に持ち出す場合は、校内教育情報セキュリティ委員会の定めるルールに則り、校長の許可の下行う。また、管理簿等に必ず記録すること。※管理簿に日時・該当教職員名・用途の他、メモリー内のファイル名を記すことが望ましい。
- ・**重要**個人私有の端末等で公的USBメモリーを使用する手順。
 - ① 使用する端末に最新のウイルス対策が施されていることを確認すること。
 - ② ネットワークを遮断する。
 - ③ 公的USBメモリーを差し、作業する。ファイル保存に際して、パスワードを設定することが望ましい。
 - ④ 学校の端末にて公的USBメモリーのウイルスチェックを行い、異常が無いことを確認後、作業をする。

- ⑤ 公的USBメモリー内のデータを消去する。
- (9) デジタルカメラ等の画像や動画で撮影に用いる一時的な記録媒体を校内専用にするとともにデータを残さないこととする。
- (10) ICレコーダ等に記録されたデータで本体内蔵の記録媒体に保存されたものは機器の中に残さないこととする。
- (11) クラウド上のドライブから端末に一旦ダウンロードしたデータは、作業終了後、端末から完全に消去しなくてはならない。
- (12) 端末を使用する業務中、止むを得ず離席する場合は、必ずスリープモードにしなければならない。

(トラブルへの対策)

- 14 ネットワークの利用において次の各号にあたるトラブルが発生した場合は、「教育情報セキュリティ対策基準」に即した対応を行う。また、必要に応じて校内教育情報セキュリティ委員会を開催し協議する。トラブルが発生した際はすぐに校長に報告をし、必要に応じて教育研究所に連絡する。校長は「教育情報セキュリティ対策基準」に即して、報告等行う。

なお、軽微な内容と判断される場合は、校長または教頭が保守点検業者に連絡する。但し、故意による機器トラブルについては保守上のサポート及び修理は受けられない。

※以下は教育委員会の整備した機器・設備・システムに限り適用される。

【重要】

ウイルス感染が疑われる場合は、真っ先にLANケーブルを端末から外すなど、即時に校内外のネットワーク（インターネット含）の接続を遮断すること。

Wi-Fi環境を利用する端末は、インターネットから端末を遮断する等、対応する。

- (1) ネットワーク機器のトラブル
- ・ コンピュータ本体 ※画面上の異常通知・見慣れない検索サイト
 - ・ プリンター
 - ・ 周辺機器等
 - ・ その他
- (2) ネットワークのトラブル
- ・ サーバやインターネットにつながらない場合
 - ・ ネットワークプリンターが使えない場合
 - ・ その他

- (3) ウイルス関係等でのトラブル
 - ・ ウイルスメールを発見した場合
 - ・ ウイルスに感染した場合
 - ・ その他
- (4) 情報モラル・エチケット等
 - ・ モラル的なことで訴えられた場合
 - ・ 子どもたち同士の中傷があった場合
 - ・ その他
- (5) その他のトラブル

(本ガイドラインの見直し及び指導)

- 15 校内教育情報セキュリティ委員会は、本ガイドラインに定めた事項について毎年見直し所属職員への指導徹底を行う。

(違反者への対応)

- 16 全ての項目に関して、「教育情報セキュリティ対策基準」に示されている内容に反しないこととする。違反者への対応については「教育情報セキュリティ対策基準」に則り、必要な措置が取られる。

(その他)

- 17 次の通知は廃止する。
 - ・ 座教指発第788号 平成21年2月27日
USBメモリによる個人情報管理について（通知）
 - ・ 座教指発第799号 平成21年3月4日
USBメモリによる個人情報管理について（通知）

附則

このガイドラインは、令和3年4月1日から施行する。