

# 菊陽町立武蔵ヶ丘中学校 情報セキュリティポリシーガイドライン（規定）

## 1 基本方針

このガイドラインは、生徒・保護者・教職員などの個人情報保護やインターネットの利用及び運営管理に関し、必要な事項を定め、適切に管理・運用するための基本的なルールを定めたものである。

## 2 対象者

対象者は、本校の業務に関わる全ての職員とする。

## 3 組織・体制

- (1) 学校長は、各校の情報セキュリティに関する権限及び責任を有する情報セキュリティ管理責任者とする。
- (2) 職員は、本情報セキュリティポリシーの内容を遵守しなければならない。
- (3) 校務分掌又は校内組織等において情報セキュリティ担当者を置く。
- (4) 情報セキュリティ担当者は、情報セキュリティ管理責任者を補佐し、各校における情報資産のセキュリティの維持、管理を行なう。
- (5) 職員には守秘義務があり、異動・退職などの場合でも、知り得た情報を漏らしてはならない。
- (6) 年度初め、情報セキュリティについて理解を図るために研修等を行う。
- (7) 情報セキュリティの維持管理を統一的な視点で行うため、情報セキュリティポリシーの策定・改案、緊急時の対応など、情報セキュリティに関する重要な事項を審議する組織として校内情報セキュリティ委員会を置く。
- (8) 校内情報セキュリティ委員会は、学校長、教頭、各学年情報教育担当、ICT支援員、生徒指導主事をもって構成する。

## 4 情報資産の管理方法

- (1) 情報資産は、業務目的の範囲内で利用すること。
- (2) 媒体・電子記録媒体等で個人情報等の重要な情報を学校外へ持ち出すことを禁止する。ただし、やむを得ない理由がある場合は、必ず事前に学校長の許可を得るとともに、「紙媒体および電子情報等の校外持ち出しに関する許可願い」に記入の上、情報漏洩対策（封入、暗号化等）を講じること。
- (3) パソコンのハードディスク内に、個人情報等の重要な情報を保存しないこと。
- (4) 個人情報・ID・パスワードなどに関する会話は、周囲に漏れることのないように十分な配慮をすること。（特に職員室内に生徒や外来者等のいる時）
- (5) 盗難や盗み見による情報漏洩を防ぐために、机上に個人情報等を放置しないようにすること。
- (6) プリンター、コピー、Faxから出力された文書は速やかに回収すること。
- (7) 情報システム機器にHDやUSBメモリ等の移動媒体を挿したままにしないこと。
- (8) 個人情報等の重要な情報が記載されている用紙を、裏紙として再利用しないこと。
- (9) 私物パソコンやタブレットの持ち込み・使用を禁止する。ただし、やむを得ない理由がある場合は必ず事前に学校長の許可を得ると共に下記の事項を遵守すること。
  - ・学校ネットワークへの接続は禁止とする。
  - ・私物パソコンやタブレットには、個人情報を含むデータを保存しない。

## 5 情報の提供（送付）について

- (1) 外部に個人情報等の重要な情報を送付する場合は、必ず事前に学校長の許可を得ること。
- (2) 情報を提供する場合は、情報漏洩対策（封入、手渡し、暗号化等）を講じること。

## **6 情報システム機器利用時の遵守事項**

- (1) 情報システム機器は、無断で改造しないこと。
- (2) 情報システム機器は、無断で他のネットワークに接続したりしないこと。
- (3) OSやソフトウェアにはセキュリティホールという情報セキュリティ上の欠陥が発見されることがあるため、使用者は出来るだけ迅速に使用している機器の最新バージョンへの更新やセキュリティパッチ（修正プログラム）を適用すること。
- (4) 個人所有の情報システム機器（ポケットWi-Fi、ルーター等）を持ち込み使用しないこと。
- (5) 情報システム機器等は、紛失・盗難防止のため、使用終了後は特定の保管場所にしまうこと。
- (6) USBメモリーやHD等の移動媒体は、随時ウイルスチェックを行うこと。

## **7 パスワード管理**

- (1) 不正アクセスを防止するため、パスワードの管理は適切に行うこと。
- (2) パスワードは、人目に触れるところに記入や貼付をしないこと。
- (3) 他人の利用者ID、パスワードを使用しないこと。
- (4) パスワードを流出してしまった場合は、速やかに学校長及び教育委員会に報告する。

## **8 ソフトウェアの取り扱い**

- (1) 私用ソフトをインストールしないこと。ただし、やむを得ない理由がある場合は、必ず事前に学校長の許可を得て必要な期間のみ使用し、使用が終わったら速やかにアンインストールすること。
- (2) ソフトウェアの違法コピーを行わないこと。
- (3) 学校がライセンス所有するソフトウェアを個人所有のパソコンにインストールしないこと。

## **9 インターネット利用時における遵守事項**

- (1) 職務に関係の無いホームページの閲覧を行わないこと。
- (2) インターネットからむやみにファイルのダウンロードを行わないこと。（業務上必要なものに限る）

## **10 電子メール利用時における遵守事項**

- (1) 職務以外の目的で電子メールを使用しないこと。
- (2) 送信時には「内容」「宛先」の確認を必ず行うこと。
- (3) 不審なメールは、開封したり、添付ファイルを実行したりしないこと。
- (4) 個人情報等の重要な情報は、メールで送信しないこと。ただし、やむを得ない理由がある場合は必ず事前に学校長の許可を得ること。なお、データそのものにパスワードをかけるか、暗号化するなどして送信すること。

## **11 コンピュータウイルスに対する遵守事項**

- (1) ウイルス感染が発覚した場合、そのパソコンのLANケーブルをすぐに外し、ウイルス対策ソフトを使用し、ウイルスの駆除又は隔離若しくは削除すると共に、学校長及び教育委員会へ報告すること。その際に使用していたUSBメモリやHD等を他で使用しないこと。

## **12 運用管理**

- (1) 学校長及び情報セキュリティ担当者は、本ポリシーが遵守されているか確認する。重大なポリシー違反が判明した場合は、迅速に対応すること。

## **13 その他**

- (1) 新たに必要な対策が発生した場合、情報セキュリティ委員会において情報セキュリティポリシーの実効性を評価し、必要な部分を見直し、内容、時期について決定を行う。この決定に基づき、情報セキュリティポリシーの更新を情報セキュリティ委員会が決定し、実施する。