制定：2025年4月1日
策定：筑波大学附属中学校 教務部

第 1 章　総則

第 **1** 条（目的） 本ポリシーは、本校における「Google Workspace for Education Plus」（以下、本サービス）を活用した情報資産の管理を適切に行い、機密性、完全性、可用性を確保することを目的とする。

第 **2** 条（適用範囲） 本ポリシーは、本校の全ての教職員を対象とし、本サービスを利用する際の情報管理とセキュリティ対策について規定する。

第 **3** 条（遵守基準） 本ポリシーは、以下の法令・ガイドラインに基づき策定する。

1. 文部科学省「教育情報セキュリティポリシーに関するガイドライン」（令和6年1月改訂）
2. 筑波大学「情報セキュリティポリシー」
3. 個人情報保護法および関連法令

第 2 章　データの分類と取扱い

第 **4** 条（生徒の画像データの取扱い）

1. 生徒の写真や動画（以下、画像データ）は、教育目的および学校広報の範囲内でのみ使用する。
2. 画像データの外部共有（Web掲載等）には、事前に保護者の同意を得るものとする。
3. 画像データの保存については、ドライブのアクセス権限設定を適切に行い、関係者外の閲覧を防ぐ。
4. 保持期間を過ぎた画像データまたは利用目的を終えたデータは、確実な方法で削除する。

第 **5** 条（データ分類とラベリング） 本サービス上に保存するデータは、以下の3区分に分類し、重要度に応じて「ドライブラベル」等を活用して管理する。

1. 機密情報**1**（要配慮情報）：成績、健康情報、指導要録に関わる個人情報（教職員・生徒・保護者等）
2. 機密情報**2**（校内情報）：授業計画、自作教材、会議資料、一般的な業務連絡
3. 機密情報**3**（公開情報）：校内掲示、学年行事案内、対外公開資料

第 3 章　セキュリティ対策

第 **6** 条（データの保存と保全／バックアップ）

1. 業務および教育活動における重要なデータは、ローカル端末（PC本体やUSBメモリ等）への保存を避け、原則として Google ドライブに保存する。
2. データのバックアップについては、手動による複製を行わず、Google Vault（データ保持機能）およびGoogle ドライブの版管理機能（バージョン履歴）によって可用性を担保する。これにより、誤削除やランサムウェア被害等からの復旧を可能とする。
3. 個人所有端末への業務データのダウンロードは原則禁止とし、業務遂行上やむを得ない場合は管理者の許可を得るものとする。

第 **7** 条（アクセス管理）

1. アカウントのID・パスワードは適切に管理し、パスワードポリシー（15文字以上等を推奨）を遵守する。
2. **2**段階認証プロセスを必須とし、不正アクセスのリスクを低減する。
3. 必要に応じてセキュリティキー（Titan Security Key等）を認証要素として活用し、より強固な対策を講じる。
4. 退職者または転出者のアカウントは、規定に基づき速やかに停止または削除する。

第 **8** 条（データ共有の制限）

1. 「機密情報1」を含むデータの共有は、必要最小限の範囲に留め、管理者の承認を得た上で行う。
2. 外部とのデータ共有は、原則として **UTOS**（または指定の校務支援システム）もしくは、適切に権限設定された Google ドライブの共有機能を活用する。パスワードを設定しないメール添付でのファイル送信は原則禁止とする。
3. 共有リンクを発行する場合は有効期限やパスワードを設定し、不要になった共有設定は速やかに解除する。

第 **9** 条（端末およびネットワーク管理）

1. 使用する端末のOSおよびブラウザは、常に最新のバージョンにアップデートする。
2. Chrome OS 以外の端末（Windows, Mac等）を使用する場合は、適切なセキュリティ対策ソフトを導入・稼働させる。
3. 端末の紛失・盗難時には、速やかに管理職および **ISIRIT**担当者 へ報告し、管理コンソールによる遠隔ロック・ワイプ等の措置を講じる。
4. 公衆無線LAN（フリーWi-Fi等）での業務利用は禁止し、校内ネットワークまたは適切な暗号化通信（VPN等）を利用する。

第 **4** 章　運用管理

第 **10** 条（管理者の責務）

1. 管理者は、Google Workspace の管理コンソールを用い、組織部門（OU）ごとの適切なポリシー適用および監査ログの確認を行う。
2. 「セキュリティセンター」等の機能を活用し、定期的にセキュリティスコアの確認とポリシーの見直しを行う。
3. インシデント発生時には、管理職および **ISIRIT**担当者 へ報告し、被害拡大の防止に努める。

第 **11** 条（インシデント対応）

1. 情報漏洩、ウイルス感染、不正アクセス等が疑われる場合、発見者は速やかに管理職および **ISIRIT**担当者 へ報告する。
2. 必要に応じて外部専門機関や筑波大学本部のセキュリティ担当と連携し、影響範囲の特定（調査ツールの活用）と対策を実施する。
3. すべてのインシデント対応の記録を作成し、再発防止のための分析を行う。
4. インシデント発生後は、影響を受けた関係者に対し、適切な情報提供および謝罪等の対応を行う。

第 **5** 章　教育・研修

第 **12** 条（教育・研修）

1. 全ての教職員に対し、本サービスの適切な利用方法と情報セキュリティに関する研修を年1回以上実施する。
2. 定期的にフィッシングメール訓練やリスク管理研修を行い、最新のセキュリティ脅威情報を共有する。

第 **6** 章　罰則

第 **13** 条（違反時の対応）

1. 本ポリシーに違反した場合、状況に応じて指導を行うほか、悪質な場合は筑波大学の規定に基づき懲戒処分等の対象となる場合がある。
2. 故意または重過失により個人情報の漏洩等の重大な損害を与えた場合、法的措置を検討する。

附則

本ポリシーは、2025年4月1日より施行する。