西都市立茶臼原小学校情報セキュリティポリシー

１　目的

学校で取り扱う情報には、児童及び保護者、教職員等の個人情報にみならず、学校教育の運営上重要な情報など､外部に漏洩等した場合には極めて重大な結果を招く情報が多数含まれている。特に近年のデジタル化された情報も多くなってきている。

しかし、デジタル化された情報はネットワークの外部からの不正アクセスや過失などにより、常に漏洩の危険と背中合わせの状態にある。

そのため、学校の情報を保護して適切に管理・運営することは重要であり、この情報セキュリティポリシーを策定、情報を取り扱う場合のルールを明確にするものである。

２　対象者

情報セキュリティポリシー対象者は、本校に係る教職員等とする。

３　セキュリティポリシーで守るもの　　※不正侵入・情報漏洩・データ改ざん等から

- ○　校務用 PC 及び USB
- ○　ユーザー ID・パスワード
- ○　メールアドレス
- ○　学校 HP・HP 登録
- ○　個人情報

・　児童の学習履歴や成績等に関する情報　　・指導の記録に関する情報 ・　保護者に関する情報　　・　教職員に関する情報　　・　身体に関する情報　等

４　体制・組織

⑴　最高責任者は校長とし、全ての情報セキュリティに関する権限及び責任を負う。

⑵　最高責任者は、教職員、児童が本ポリシー、最高責任者及び情報管理者の指導を守らない場合に、利用させないことができる。

⑶　本校職員は、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。

⑷　校務分掌又は校務組織において、情報管理者（教頭）と情報セキュリティ担当者（情報教育担当）を置く。

⑸　教職員には守秘義務があり、異動・退職などの場合、知り得た情報を漏らしてはならない。

⑹　年度初め、情報セキュリティの研修を行う。

５　情報管理及び機器、ネットワーク管理等

⑴　一般管理

使用していない書類や記録媒体は机の引き出し、キャビネット等に収納し、机上に放置しない。不必要になった書類等は、シュレッダーにて確実に廃棄する。

⑵　校務用 PC 管理

ア　情報管理者（教頭）は、出勤時に PC 保管用キャビネットを解錠し、退勤時に施錠する。

イ　校務用 PC は、出勤時に PC 保管用キャビネットから取り出し、退勤時に収納する。

ウ　原則として、児童の重要情報は校務用 PC で作成する。

エ　私物の PC の使用は原則禁止とする。私物 PC を使用する場合、情報管理者（教頭）の許可を得ると共に下記の事項を遵守しなければならない。

○　校内ネットワークへの接続は禁止とする。 ○　私物 PC は、ウイルス対策ソフトをインストールした上で、常時ファイル更新を行い、最新の状態にしておく。

オ　校務用 PC の校外への持ち出しは禁止とする。

カ　校務用 PC にファイル交換ソフトをインストールしてはならない。

キ　外部の者が校務用 PC を起動し、データを参照することは厳禁とする。但し、業者によるメンテナンスについては、情報管理者（教頭）の許可を得てからとする。

⑶　データ（USB 等）管理

ア　校務用 USB は、PC 保管用キャビネットに保管し、必要な場合に取り出し使用する。

イ　情報セキュリティ担当者（情報教育担当）は、定期的に校務用 USB の保管状況を確認する。

ウ　重要な個人データを USB 等の外部記憶装置に保存し、校外に持ち出すことは原則禁止とする。但し、やむを得ず持ち出す場合には、情報管理者（教頭）の許可を得ると共に、下記の事項を遵守しなければならない。

○　持ち出し記録簿に、目的や場所等を記載する。
○　パスワードをかけ、紛失・盗難などの事故による情報漏洩を防止する。
○　自宅等でデータを使用する場合は、複製したデータがインターネット等を通して漏洩することがないよう、私物 PC のセキュリティを保持する。
○　自宅等でデータを更新した場合は、校務用 USB に保存し、私物 PC 等に保存しない。
○　持ち出したデータが盗難もしくは紛失した場合、又は、インターネット等を通して漏洩した場合は、速やかに情報管理者（教頭）に報告し、指示を仰ぐ。

エ　児童に関する指導要録、名簿、成績等のデータをコピー又は印刷して校外に持ち出すことは原則禁止とする。やむを得ず持ち出す場合には、情報管理者（教頭）の許可を得る。

オ　児童の重要情報は、校務用 PC のデスクトップやハードディスクではなく、メイン PC（サーバー機）に保存し、校内 LAN でデータを共有する。

⑷　パスワード管理

ア　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。

イ　パスワードは、人目に触れるところに記入や貼付してはならない。

ウ　他人の ID、パスワードを使用してはならない。

⑸　ソフトウエア・周辺機器

ア　校務用 PC に、ソフトウエアを勝手にインストールしてはならない。

イ　ソフトウエアを不正にコピーしてはならない。

⑹　ウイルス対策

ア　不審なメールに添付されたファイルは、決して開かず削除する。

イ　ファイルを添付して送信する場合には、ウイルス感染の無いことを確認しなければならない。

⑺　インターネット・メールの管理

ア　インターネットの利用は、校長の責任のもとで行うものとする。

イ　インターネットやメールの使用は、教育活動での利用（学習活動や児童の情報活用能力の育成、指導上の資料の収集、情報交換等）に限定し、教育の推進や向上を目的として行う。

ウ　教職員は、人権尊重、個人情報の保護、著作権等に配慮し、インターネットの活用法については、児童の発達段階に応じ、適切に指導すると共に、児童の情報モラルの育成を図る。

⑻　HP の開設・情報発信

ア　学校 HP は、学校の教育活動を主体として作成し、校長の許可を得た上で公開する。

イ　HP に掲載した情報については、校長が責任を負う。

ウ　HP の発信は、情報管理者（教頭）又は情報管理者（教頭）から委任されたものが中心となって行うが、全職員が作成することができる。

エ　教職員は、不特定多数による閲覧があることを十分にふまえ、ページを作成する。

オ　児童の写真、作品等の掲載については、以下の点に留意する。

○　年度初めに集約した「個人情報に係る保護者の同意」表を確認し、掲載する。
○　国籍・本籍・住所・氏名・電話番号・生年月日・家族構成等は掲載しない。

カ　著作権

○　掲載する情報

文章、絵画、写真、音楽等はその著作権に十分配慮しなければならない。

○　本校の著作権

トップページに学校の著作権を明記する。

○　児童作品には、著作権を明記する。

「無断で配付、転用、加工することを禁じます。校長」

６　トラブル時の対応

○　コンピュータ等の機器トラブル、ネットワークに関するトラブル、ウィルス感染時の対応については、いずれの場合も委託業者（学教）に連絡する。

⑴　迷惑メール（嫌がらせメール）に対する対応

迷惑メールを送信拒否するために返信や差出人不明のメールに返信することは、相手に不必要な情報を提供することになるので、基本的には無視する。

⑵　学校のホームページの改ざん等への対応

不正アクセスなので、速やかに教育委員会及び委託業者に連絡する。

⑶　個人情報の漏洩に関する対応

ア　校務用 PC に個人情報を保存すると、不正アクセスで漏洩したり、児童がその内容を偶然見たり、故意に CDR や USB メモリ等に保存して外部に持ち出したりする原因となるので、校務用 PC には絶対に個人情報を保存しない。

イ　情報の漏洩は、外部からの指摘で分かることが多いが、その時点ですでに手遅れとなり重大な問題となることがある。日頃から細心の注意・配慮が必要である。

７　その他（禁止事項等）

⑴　インターネットで発信する内容について、言語、表現方法、内容等、人権に係る表現を考慮しなければならない。

⑵　メールを送信する場合は、相手に迷惑をかけないためにも、メールの添付ファイルの容量を小さくするように努める。（最大２ MB 似内）

⑶　非合法な情報や公序良俗に反する情報等を送受信してはならない。

⑷　法令に違反するもの、また違反する恐れがある行為をしてはならない。

⑸　最高責任者（校長）は、サーバーを管理し、サーバーの教育ネットワーク等に関わる設定の変更を認めない。

⑹　教職員、児童はネットワーク等のセキュリティを侵害する行為をしてはならない。

⑺　上記の定めるものの他は、別途最高責任者（校長）が定める。

⑻　本情報セキュリティポリシーガイドラインは、必要に応じて見直し、更新するものとする。

（更新月日）　平成３１年４月１日