情報セキュリティガイドライン

（趣旨）

第１条　このガイドラインは、情報漏えい対策に関する規程に基づき、学校法人聖徳学園（以下「学園」という。）の保有する情報（以下「機密情報等」という。）、及び個人情報や個人データ、個人保有データ（以下「個人情報等」という。）を取り扱う情報機器及び情報媒体の適切な管理についての指針を定めるものとする。

（用語の定義）

第２条　このガイドラインにおいて、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

（１）　情報機器とは、デスクトップ型ＰＣ、ノート型ＰＣ、タブレット型端末、携帯電話等の機密情報等及び個人情報等を取り扱う機器をいう。

（２）　構成員とは、職員等及び学生生徒等をいう。

（３）　利用者とは、情報機器及び情報媒体を利用して、機密情報等及び個人情報等を取り扱う学園の構成員をいう。

（４）　管理者とは、学園すべての管理職員をいう。

（５）　情報媒体とは、情報記憶媒体及び情報通信媒体、並びに情報紙媒体をいう。

ア　情報記憶媒体とは、機密情報等及び個人情報等を保存したハードディスク（ＨＤＤ：内蔵型、外付型及び携帯型を含む。）、ＣＤ、ＤＶＤ、ＭＯ、ＵＳＢメモリ、メモリカード、磁気テープ等情報の書き込み、再生及び読み取りの可能なすべての電磁的、光学的記憶媒体をいう。

イ　情報通信媒体とは、電子メール、電子ニュース、Ｗｅｂシステムなどのインターネットやサーバ等を使用する通信手段をいう。

ウ　情報紙媒体とは、機密情報等及び個人情報等を記載した紙及び紙に準じた記録物をいう。

（６）　ウイルス等とは、メッセージの表示、ファイルの破壊、情報の漏えい等を実行する機能を持った不正なコンピュータプログラムをいう。

（７）　完全消去とは、電子データ及び紙媒体を復元不可能な状態にして、再利用できない状態にすることをいう。

（８）　ファイル交換ソフトとは、Winny 等に代表されるネットワークを介して不特定多数のコンピュータの間でファイルを交換するソフトをいう。

（適用範囲）

第３条　学園の事業を維持・発展させる上で、「機密性、完全性及び可用性」が損なわれた場合に学園に損害を与える情報を扱うすべての情報機器及び情報媒体の利用行為を適用範囲とする。

（組織体制）

第４条　機密情報等及び個人情報等を取り扱う情報機器及び情報媒体のセキュリティに関する責任者は、各学校の所属長とする。

（情報機器利用遵守事項）

第５条　利用者は、機密情報等及び個人情報等を取り扱う情報機器に関し、次の各号に掲げる事項を遵守して管理する。また、同事項が遵守されていない、又は遵守されているかどうか不確かな情報機器（例えば、他の者の管理する情報機器、インターネットカフェ等で不特定の者が利用する情報機器）では、情報の取り扱いを禁止する。

（１）　パスワードによる管理

情報機器には第三者に類推されにくいパスワードを設定し、取り扱いには十分留意する。

（２）　クリアスクリーンによる管理

ア　離席時は、コンピュータのロック又はログオフを行い、不正な操作又は画面の盗み見を防止する。画面設定では、パスワード付きスクリーンセーバが動作するように設定する。

イ　持ち運びや移動が可能な情報機器（ノート型ＰＣ、タブレット型端末 等）を帯出して使用する場合は、第三者から盗み見が可能な環境では使用しない。

ウ　作業終了時は、使用した情報機器の電源をオフにする、又は利用再開時にパスワード等の認証が必要とされる状態にする。

（３）　持ち運びや移動が可能な情報機器の管理

ア　持ち運びや移動が可能な情報機器の保管は、個室、ロッカー、引出し等の施錠可能な設備での施錠保管、盗難防止ワイヤー等での固定保管等、盗難対策を実施する。

イ　持ち運びや移動が可能な情報機器を帯出して使用する場合は、事前に管理者の許可を得た上で、紛失、盗難、破損等の防止に十分留意する。

（４）　アカウントによる他の者の利用の制限

他者（構成員、またその親族を含む。）の無断使用防止するため、アカウント及びパスワードの設定を行う。また、他者に利用させる場合は、管理者権限の設定等、適切な制限下で利用させる。

（５）　ソフトウェアインストールの制限

機密情報等及び個人情報等を保存する情報機器について、ファイル交換ソフトウェア等情報漏えいの危険性のあるものについては、これを禁止する。詳細については各学校の作成するハンドブック等に定める。

（６）　時刻合わせ

各種の記録等に利用するため、常に情報機器の時刻は正しく合わせる。

（ウイルス対策）

第６条　利用者は、次のとおり、ウイルス対策を行う。

（１）　感染防止手順

ア　学園の推奨するウイルス対策ソフトウェアをインストールし、ウイルス対策が有効な状態で利用する。

イ　ネットワーク、情報媒体等により外部から入手するファイルに対しては、自動検知機能（リアルタイムスキャン）を有効にする。

ウ　ウイルス対策ソフトウェアの定義ファイルは、継続的に更新を行う。

エ　オペレーティングシステム等の修正プログラム（Windows Update 等）が頒布されている

場合は、適宜これをインストールする。

（２） ウイルス感染時の対応

ウイルス等の感染を発見した場合、又はウイルス対策ソフトウェアが不正なプログラムの除去・隔離に失敗した場合は、感染した情報機器を直ちにネットワークから物理的に切り離し、速やかに管理者へ報告するとともに、大学情報教育研究センターへ報告し、必要に応じて指示を求める。

（情報記憶媒体利用遵守事項）

第７条　利用者は、機密情報等及び個人情報等を保存した情報記憶媒体に関し、次の各号に掲げる事項を遵守して管理する。

（１） 機密情報等及び個人情報等を保存した情報記憶媒体は、施錠可能なキャビネット等の設備に施錠保管し、不在にする際は必ず施錠する。

（２） 機密情報等及び個人情報等を保存した情報記憶媒体を持ち運ぶときは、事前に管理者の許可を得た上で、紛失、盗難、破損等からの防止に十分留意する。

（情報通信媒体利用遵守事項）

第８条　利用者は、機密情報等及び個人情報等を有する情報通信媒体に関し次の各号に掲げる事項を遵守して管理する。

（１） Web 利用時

ア　Web サイトへ個人情報等（メールアドレス、氏名、所属 等）を入力するときは、通信の暗号化（https://）を確認する等、十分注意を払う。

イ　Web サイトには、ウイルス等を感染させる又はセキュリティ上危険なソフトウェアを実行させるものがあるため、ブラウザのセキュリティレベルを「中」以上に設定する等、その利用には十分注意を払う。

（２） ブログやソーシャルネットワークサービス（以下「ＳＮＳ」という）の利用

ア　ブログやＳＮＳ等でのコミュニケーションや情報発信の際には、他者のプライバシー、個人情報、名誉、肖像、著作、商標といった人格権、財産権を毀損または侵害しないよう、必要に応じて個人や権利者の許諾を得るとともに、関連の法令を遵守する。

イ　情報の信憑性、正確性について十分吟味のうえ、情報発信するよう心がける。また、情報発信後に誤りが判明した場合には、可能な限り情報の訂正や抹消につとめる。

ウ　その他、学園及び学園の構成員の権利や利益を不当に侵害する情報を発信しない。

（３） 電子メール利用時

ア　電子メールのアドレスを入力するときは、宛先を十分確認し、送信前には、宛先、ｃｃ、ｂｃｃを必ず確認する。（ｃｃで送信する場合、受信者のアドレスが表示されるため、特に注意が必要。）

イ　個人情報等を含む電子情報を電子メールにて送信する場合、機密情報等及び個人情報に暗号化を実施した電子ファイルを添付するものとする。この際、復号に必要なパスワードは、別の手段で連絡する。

（情報紙媒体利用遵守事項）

第９条　利用者は、機密情報等及び個人情報等を含む情報が記載されている情報紙媒体に関し、次の各号に掲げる事項を遵守して管理する。

（1）　機密情報等及び個人情報等を含む情報が記載されている情報紙媒体は、施錠可能な室内に保管し、不在にする際は必ず施錠する。

（2）　機密情報等及び個人情報等を含む情報が記載されている情報紙媒体を持ち運ぶときは、事前に管理者の許可を得た上で、紛失、盗難、破損等の防止に十分留意する。

（電子ファイルの取り扱い）

第 10 条　利用者は、電子ファイルについて、次のとおり取り扱う。

（1）　機密情報等及び個人情報等を含む電子ファイルを帯出するときは、帯出の方法によらず、保存時に電子ファイルの暗号化を行う。

（2）　電子ファイルの暗号化を行うときは、復号に必要なパスワードを、類推されにくいものとする。

（情報記憶媒体の保管、移送等の外部委託）

第 11 条　機密情報等及び個人情報等が保存されている情報記憶媒体の保管、又は移送を外部業者に委託する場合の対応は、次のとおりとする。

（1）　機密情報等及び個人情報等が保存されている情報記憶媒体の保管を外部倉庫業者等に委託する場合は、安全管理の要求を十分に満たす業者を選定し、契約を締結した上で実施する。

（2）　機密情報等及び個人情報等が保存されている情報記憶媒体の移送は、手渡しで行う、あるいは信頼できる輸送手段及び輸送会社を選定し、委託する。

（3）　機密情報等及び個人情報等が保存されている情報記憶媒体の輸送を委託する場合は、郵便にあっては、書留郵便を、宅配便等にあっては、重要物運搬便等（集荷から配達までを記録し、紛失又は損失時に一定の保証があるもの）必ず輸送記録が可能なものを利用する。

（4）　輸送中の事故に備え、輸送する情報のバックアップを保管する。

（5）　電子メールを用いる場合は、第８条（3）項のイに準ずる。

（情報紙媒体の保管、移送等の外部委託）

第 12 条　機密情報等及び個人情報等が記載されている情報紙媒体は、施錠可能な室内に保管し、不在にする際は必ず施錠する。また、移送する場合は、次のとおり対応する。

（1）　機密情報等及び個人情報等が記載されている情報紙媒体の保管を外部倉庫業者等に委託する場合は、安全管理の要求を十分に満たす業者を選定し、契約を締結した上で実施する。

（2）　機密情報等及び個人情報等が記載されている情報紙媒体の移送は、手渡しで行う、あるいは信頼できる輸送手段及び輸送会社を選定し、委託する。

（3）　機密情報等及び個人情報等が記載されている情報紙媒体の輸送を委託する場合は、郵便にあっては、書留郵便を、宅配便等にあっては、重要物運搬便等（集荷から配達までを記録し、紛失又は損失時に一定の保証があるもの）必ず輸送記録が可能なものを利用する。

（情報機器の廃棄等）

第 13 条　機密情報等及び個人情報等が保存されている電子ファイルについては、サーバに保存して利用するよう十分留意し、一時的に別の情報機器に保存する必要がある場合は、利用後速やかに完全消去する。

２　機密情報等及び個人情報等を含む電子ファイルが、現に保存されている、若しくは保存されていた情報機器を廃棄、返却又は譲渡する場合の対応は、次のとおりとする。

（１）　情報機器の廃棄を行うときは、ハードディスクの情報を完全消去し、又はハードディスクを物理的に破壊（後者が望ましい。）する。

（２）　情報機器の返却又は譲渡を行うときは、ハードディスクの情報を完全消去する。

（３）　情報機器のハードディスクの情報の消去を外部業者等へ委託するときは、守秘義務等の契約を締結した上で実施し、完全消去を保証する文書等の発行を依頼する。

（４）　情報機器の廃棄、返却又は譲渡において、自らハードディスクの情報の完全消去が困難な場合は、大学情報教育研究センターに支援を要請し、大学情報教育研究センターがハードディスクの情報の完全消去を行う。その際、担当者は、情報へのアクセスを必要最小限とし、知り得た情報を公開又は利用してはならない。

（情報記憶媒体の廃棄等）

第 14 条　機密情報等及び個人情報等を含む電子ファイルが、現に保存されている、若しくは保存されていた情報記憶媒体を廃棄する場合は、情報の完全消去又は情報記憶媒体の破壊若しくは裁断処理を行い、返却又は譲渡する場合は、情報の完全消去を行う。

（情報紙媒体の廃棄等）

第 15 条　機密情報等及び個人情報等が記載されている情報紙媒体を廃棄する場合は、裁断、焼却、溶解等により処分する。

（学校単位のハンドブック等の作成）

第 16 条　各学校は、本ガイドラインに基づいて、情報の取り扱いに関するハンドブック等を作成し、情報の適切な取り扱いを奨励する。

附　　則

このガイドラインは、平成 27 年 4 月 1 日から施行する。