坂出第一高等学校　情報セキュリティポリシー

（平成２８年４月１日施行の「情報セキュリティ実施手順」と
平成３１年４月１日施行の「情報セキュリティポリシー」を融合させた内容です。）

第１章　総則

（目的）

第１条　このポリシーは，坂出第一高等学校（以下，「学校」という。）におけるネットワーク及び情報機器等の利用に係る運用管理並びに電子的情報の管理について，必要な事項を定め，校務及び教育の情報化を推進するとともに，情報セキュリティの確保に資することを目的とする。

（用語の定義）

第２条　このポリシー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）教職員　　学校の教職員（非常勤講師を含む。）をいう。

（２）ネットワーク　　学校が整備した情報ネットワーク（クラウドを含む。）をいう。

（３）情報機器等　　サーバ，パーソナル・コンピュータ（以下，「パソコン」という。）及びプリンタ等の情報処理を行う機器並びにルーター（ファイアウォールを含む。），ハブ等のデータ通信を行う機器をいう。

（４）端末等　　ネットワークに接続して利用するパソコン及び接続せず単独で利用するパソコンをいう。

（５）利用者　　情報機器等を利用する者をいう（生徒を含む。）。

（６）電子メールアカウント　　電子メールを送受信するための個人情報及び権限をいう（電子メールアドレスを含む。）。

（７）ユーザＩＤ　　利用者及び所属等に与えられる利用者識別のための文字列をいう。

（８）パスワード　　利用者の情報保護のため，ユーザＩＤごとに設定する暗証用文字列をいう。

（９）インストール　　ソフトウェア（以下，「ソフト」という。）を情報機器等に導入することをいう。

（１０）ウイルス　　プログラムやデータに対して意図的に何らかの被害を及ぼすように作られたプログラムであり，自己伝染機能，潜伏機能及び発病機能のいずれかの機能を有するものをいう。

（１１）ＭＡＣアドレス　　機器固有情報等の識別コードをいう。

（１２）記録媒体　　ハードディスク，ＣＤ，ＤＶＤ，ＢＤ等，データを記録しておくための装置（ＵＳＢメモリ，紙媒体を除く。）をいう。

（１３）ネットサーバ　　学校に設置されている情報通信ネットワークのサーバをいう。

（対象範囲）

第３条　このポリシーの対象範囲は，本校の施設及び本校が保有するすべての情報資産である。

（適用）

第４条　このポリシーは，勤務形態を問わず，本校の全教職員に適用される。

（総括責任者の職務）

第５条　校長を情報セキュリティー総括責任者（以下,「総括責任者」という。）とし，学校内での利用に関して次の職務を行う。

（１）学校内の情報化に関する企画及び推進に関すること。

（２）ネットワーク及び情報機器等の利用に係る総括的な運用管理に関すること。

（３）学校内の情報資産の管理を総括すること。

（４）教職員の情報化に係る啓発，研修及び訓練に関すること。

２　総括責任者は，副校長１名，教頭１名及び事務部長を，情報セキュリティ管理者（以下,「管理者」という。）として選任するものとする。

３　総括責任者は，教職員から２名以上の者を情報セキュリティ推進員（以下,「推進員」という。）として選任するものとする。

（管理者の職務）

第６条　管理者は，次の職務を行う。

（１）総括責任者の職務を補佐すること。

（２）総括責任者の指示に基づき，学校内の情報化，ネットワーク及び情報機器等の利用並びに電子的情報の管理について,推進員に対して具体的な指導及び助言を行うこと。

（推進員の職務）

第７条　推進員は，次の職務を行う。

（１）学校内の情報化，ネットワーク及び情報機器等の利用並びに電子情報の管理に関する教職員への指導に関すること。

（２）障害時における連絡及び一次対応に関すること。

（３）その他，管理者の指導及び助言に基づく職務を行うこと。

（教職員の責務）

第８条　教職員は，就業規則第３０条第３号及び第４号を遵守するとともに，このポリシーの趣旨を十分に理解し，遵守しなければならない。

２　教職員は，ネットワーク及び情報機器等を職務以外に利用してはならない。

（情報化推進委員会の設置）

第９条　総括責任者を委員長とする情報化推進委員会を設置する。

２　委員には，管理者，推進員，その他をもって充てる。

３　情報化推進委員会は，次の事項を実施する。

（１）情報化に関する企画及び推進について具体的な検討を行うこと。

（２）ネットワーク及び情報機器等の利用に係る運用管理並びに電子的情報の管理の具体的な手順（以下,「実施手順」という。）を策定すること。

（３）実施手順の運用状況について審議し，必要に応じて実施手順の見直しを行うこと。

（実施手順）

第１０条　情報化推進委員会が策定することとされる実施手順には，次の各号に掲げる事項を定めるものとする。

（１）第２１条に規定する情報機器等の具体的な管理方法

（２）第２２条並びに第２３条に規定する情報資産の分類とその具体例

（３）第２４条並びに第２５条に規定する情報資産の取り扱いランクの分類とその具体例

（４）第２６条に規定する情報資産を取り扱う際の留意点

（５）電子メールアカウント，ユーザＩＤ及びパスワードの管理方法

（６）その他このポリシーの規定を実施するために必要な事項

第２章　ネットワーク及び情報機器等の運用管理

（利用内容）

第１１条　ネットワーク及び情報機器等は，次の用途で利用することができる。

（１）学校教育活動を行うための利用

（２）校務を処理するための利用

（３）総務事務処理のための利用

（学校内で利用できるサーバ及び端末等）

第１２条　学校内で利用するサーバ及び端末等は，次の各号のいずれの要件も満たすものでなければならない。

（１）学校が管理するものであること。

（２）ウイルス対策ソフトがインストールされていること。ただし，Windows 系ＯＳ以外のＯＳを利用したサーバ及び端末等で，有効なウイルス対策ソフトが存在しない場合は，これに準ずる対策がなされていること。

（３）ファイル交換ソフト（インターネットを介して不特定多数のコンピュータの間でファイルを共有するソフトをいう。），著作権法に違反するおそれがあるソフト又は特定のサーバに負荷を与えるソフトがインストールされていないこと。

２　個人所有端末等については，前項第２号及び第３号の要件を満たし，かつ，個人所有端末等利用申請書（様式１）により総括責任者又は管理者（以下，「総括責任者等」という。）の許可を得た場合に限り，職務を行うに際し学校内で利用することができる。

３　個人所有端末等は，ネットワークに接続してはならない。ただし，総括責任者等が許可した場合には，生徒向け端末用のネットワークに接続することができる。

４　学校内で利用する個人所有端末等の所有者は，当該端末等が第１項第２号及び第３号の要件を満たすことを証明する責を負うものとする。

（学校が整備したもの以外のソフトのインストール）

第１３条　情報機器等へ新たにソフトを追加インストールする場合は，ソフトウェアインストール申請書（様式２）を総括責任者に提出して，その許可を得なければならない。

２　申請者が前項の許可を受けてインストールしたソフトの保守及び管理は，当該申請者

が行うものとする。

（無線回線の利用）

第１４条　学校内で無線回線を利用する場合は，次の措置を講じるものとする。

（１）接続しようとする端末等を，ＭＡＣアドレスで自動的に判別する等の措置を，情報機器等に講じること。

（２）可能な限り高いレベルの暗号化の措置を講じ，暗号化キーは厳重に管理すること。

（不正アクセス対策）

第１５条　推進員は，不正アクセスを防止するため，次の措置を講じるものとする。

（１）メーカー等から提供される修正プログラム等を速やかに適用すること。

（２）ネットワーク内の情報機器等からの不正アクセスが発見された場合，直ちに総括責任者等に報告し，情報機器等の切断及び不正アクセスを行った者の特定等，適切な処置を求めること。

（ウイルス対策）

第１６条　推進員は，ウイルスに関する情報の収集に努め，教職員に対して最新の情報を提供するとともに，適切なウイルス対策を講じるよう指導するものとする。

２　サーバ及び端末等を利用する教職員は，ウイルス対策を行うため，次の措置を講じるものとする。

（１）サーバ及び端末等において，定期的なウイルスチェックを行うこと。

（２）ウイルス対策ソフトは，常に有効な状態を保つとともに，ウイルスチェックに用いるウイルス定義データベースが最新のものであることを確認すること。

（３）推進員が提供するウイルス情報に常に留意すること。

（４）外部から持ち込まれた記録媒体を利用する場合は，あらかじめ必ずウイルスチェックを行うこと。

（５）サーバ及び端末等がウイルスに感染していることが判明した場合には，直ちにネットワークから切断した上で，推進員に報告し，その指示に従って適切な措置を講じること。

（パスワードの管理）

第１７条　パスワードは相当の文字数とし，文字列は他の者が推測しにくいものでなければならない。

２　推進員は，適切にパスワードを管理するため，次の措置を講じるものとする。

（１）パスワードを新規に発行する場合は，仮のパスワードを発行し，ログイン後，直ちに教職員にパスワードを変更させること。

（２）必要に応じてパスワードの設定状況を調査し，不適正な使用を行っている教職員には，速やかに是正させること。

（３）パスワードを保管するファイルは，利用者以外の者が入手できないように暗号化を施す等，適切に管理すること。

３　利用者は，適切にパスワードを管理するため，次の措置を講じるものとする。

（１）パスワードは秘密にし，他の者に知られないようにすること。

（２）パスワードが他の者に知られた場合，又はそのおそれがある場合は，パスワードを速やかに変更すること。

（３）過去に使用したパスワードを再利用しないこと。

（ファイルの共有）

第１８条　推進員は，学校内でファイル共有を行う場合は，パスワードやアクセス権限を設定するなど，ファイルを利用する権限のある者だけが利用できる仕組みを策定するものとする。

（インターネットの利用）

第１９条　利用者は，次の事項に留意してインターネットを利用するものとする。

（１）インターネットのアクセスにあたっては，職務に限定すること。

（２）ソフトウェア，ファイルをダウンロードする場合は，ウイルス等のチェックをした上で行うこと。

（３）パスワードをＷｅｂブラウザに記憶させないこと。

（電子メールの利用）

第２０条　利用者は，次の事項に留意して電子メールを利用するものとする。

（１）電子メールの送受信は，職務に限定すること。

（２）生徒及び教職員の個人情報に関わる情報は，電子メールを用いて送信しないこと。

（３）電子メールに添付されたファイルは，必ずウイルスチェックを行うこと。

（４）電子メールの自動転送機能は，職務上特に必要な場合を除いて，利用しないこと。

（５）電子メールアカウントは，総括責任者の指示のもと推進員が発行したもののみを利用すること。

（６）不審なメール等については，開封せずに削除等を行う。

（情報機器等及び記憶媒体の管理）

第２１条　総括責任者は，情報機器等及び記憶媒体の管理にあたっては，盗難防止のための措置を講じなければならない。

２　利用者は，使用する情報機器等及び記憶媒体について，他の者が無断で使用又は情報を閲覧することができないよう適切に管理しなければならない。

３　記憶媒体としてＵＳＢメモリーの使用は禁止する。

第３章　ネットワーク及び情報機器等における情報資産の管理

（情報資産の分類）

第２２条　本校が所有する情報資産を構成する情報要素を次の通り分類し，情報資産を管理する。

分類Ⅰ　　成績結果，進路状況，人物・行動記録，健康状態，家庭状況に関する個人情報（セキュリティ侵害による，生徒及び保護者へ及ぼす影響が，重大な個人情報）

分類Ⅱ　　入試実施要領，情報セキュリティポリシー（セキュリティー侵害による，学校運営等への影響が，重大な業務等情報）

分類Ⅲ　　その他の個人情報（セキュリティ侵害による，生徒及び保護者へ及ぼす影響が，比較的軽微な個人情報）

（分類の具体例）

第２３条　情報要素の分類による具体例は，次の通りである。

	具体例	分類				具体例	分類		
		Ⅰ	Ⅱ	Ⅲ			Ⅰ	Ⅱ	Ⅲ
基本情報・家庭情報	氏名			○	出欠情報	欠席日数等	○		
	生年月日			○		欠席理由等	○		
	保護者名			○	進路情報	受験校	○		
	出身中学校			○		合否情報	○		
	住所			○		進学・就職先	○		
	電話番号			○	保健情報	身体情報	○		
	通学方法			○		健康情報	○		
	部活動			○		病歴	○		
	学級役員			○	指導情報	進路指導記録	○		
	生徒顔写真			○		教科指導記録	○		
	家庭の状況	○				生徒指導記録	○		
成績情報	定期考査成績	○				教育相談記録	○		
	業者テスト成績	○				賞罰記録	○		
	その他テスト成績	○				在籍記録	○		
	課題等提出状況	○				行動記録・人物評	○		
	答案用紙	○			学校運営	入試実施要領		○	
	高校入試成績	○				情報セキュリティポリシー		○	

（取り扱いランクの分類）

第２４条　本校が所有する情報資産の取り扱いランクを以下の通り分類し，情報資産を管理する。

取り扱いランク	内　　容	取り扱い
A	分類Ⅰの情報要素を含む個人情報	持ち出し禁止
B	分類Ⅱの情報要素を含む業務情報及び分類Ⅲの情報要素を含む個人情報が，一定量（１学年分）以上集合したもの	持ち出し原則禁止（総括責任者が個別承認）
C	分類Ⅲの情報要素を含む個人情報で，一定量（１学年分）に満たないもの	持ち出し要注意

（分類の具体例）

第２５条　情報資産の取り扱いランクの分類による具体例は，次の通りである。

分掌等	具体例	取り扱いランク		
		A	B	C
教務部	生徒指導要録	○		
	成績一覧表	○		
	出席簿	○		
	住所録		○	
	奨学金関係資料	○		
	転出入関係書類	○		
	成績会議等資料	○		
	入試関係資料	○		
	入試実施要領		○	
生徒指導部	生徒名簿・写真		○	
	生徒指導委員会資料	○		
	非行報告書	○		
	各種許可願	○		
	生徒指導記録簿	○		
	懲戒台帳	○		
進路指導部	業者テスト成績	○		
	進路検討会資料	○		
教育相談部	心理検査等結果	○		
	教育相談面接等結果	○		
保健関係	保健調査票関係	○		
	健康診断票関係	○		
	保健室利用状況記録	○		
	学校保健日誌	○		
	日本スポーツ振興センター災害報告書	○		
	生徒成績	○		
	進路指導・生徒指導記録	○		
	調査書	○		
	推薦書	○		
	クラス･部活動等名簿			○
	クラス･部活動等住所録			○
	クラス･部活動等緊急連絡網			○
	教務手帳（注）		○	
	答案用紙（注）		○	
	課題・提出物			○
	情報セキュリティポリシー		○	
	その他「分類Ⅰ」の情報要素を含む個人情報	○		
	その他「分類Ⅱ」の情報要素を含む業務等情報及び分類Ⅲの情報要素を含む個人情報（１学年分以上の数量のもの）		○	
	その他「分類Ⅲ」の情報要素を含む個人情報（１学年未満の数量のもの）			○

（注）教務手帳及び答案用紙には「分類Ⅰ」の情報が含まれるが，職務上持ち出しの必要が生じるものであるため，例外的に「Ｂ」ランクの扱いとする。

（情報資産を取り扱う際の留意点）

第２６条　利用者は，情報資産の取り扱いに関して，次のことに留意すること。

（１）バックアップを定期的に行うこと。

（２）ユーザＩＤ，パスワードの設定等，情報を利用する権限のある者だけが利用できるよう必要な措置を講じること。

（３）個人情報を取り扱う場合は，当該個人情報の重要度に応じたアクセス権限を設けること。

（４）個人情報を含む情報については，すべてのファイルにパスワードを設定するとともに，必要に応じてファイルまたはフォルダの暗号化を行うこと。
（５）情報資産を記録した記憶媒体は，施錠が可能な場所に保管すること。
（６）退職をする場合は，個人情報を含むすべての情報（後任者に引き継ぐ必要がある情報を除く。）について，情報を復元できないように消去すること。
（７）情報資産を記録した記憶媒体は，総括責任者の指示により保存期間満了後に廃棄するとともに，廃棄する場合は，当該情報を復元できないように消去し，又は記録媒体を破砕すること。
（８）情報機器等を外部の者に修理させる場合は，情報資産を復元できないように消去するものとする。ただし，消去できない場合は，当該外部の者に対して守秘義務を課した上で，修理させること。
（９）情報機器等を賃借期間の満了に伴い外部の者に返却する場合，又は情報機器等を廃棄する場合には，情報資産を復元できないように消去するものとする。ただし，消去できない場合は，当該外部の者又は廃棄を依頼する者に対して，守秘義務を課した上で，当該情報を復元できないように消去させ，又は当該情報を記録した媒体を破砕させること。
２　生徒等の個人情報の漏えい等が発生又は判明した場合については，総括責任者等へ報告すること。

（情報の持ち出しの禁止）

第２７条　第３章で規定された情報資産又はパソコンを，学校外へ持ち出さないこと。ただし，職務の遂行上，やむを得ず持ち出さざるを得ない場合は，情報資産又はパソコン持ち出し申請書（様式３）により，総括責任者等の許可を得なければならない。
２　総括責任者等は，前項の許可を受けようとする者が，次の事項を遵守することを確認した上で，許可を行うものとする。
（１）持ち出す情報は，必要最小限にすること。
（２）記録媒体を用いる場合は，学校が許可したセキュリティの条件を満たしたものを使用すること。
（３）寄り道など，申請した持ち出し先以外の場所に情報を持ち出す行為やパソコン及び記録媒体の放置をしないこと。
（４）申請したパソコン又は記録媒体以外に情報をコピーしないこと。
（５）パソコンを起動したまま放置して，他の者に利用されることのないこと。
（６）作業は，パソコンを外部ネットワークから切り離した状態で行うこと。
（７）持ち出した情報は，以下の条件を満たすパソコンであること。
ア　ウイルス対策ソフトがインストールされ，かつ，ウイルス定義データベースが最新の状態に保たれているパソコンであること。
イ　ファイル交換ソフト又は著作権法に違反するおそれがあるソフトがインストールされていないパソコンであること。
ウ　ユーザＩＤ・パスワードを設定したパソコンであること。
エ　ＯＳが最新の状態に保たれたパソコンであること。
（８）持ち出しに使用したパソコン又は記録媒体を学校に持ち帰った時は，ウイルスチェックを行うこと。
３　総括責任者は，学校外での作業完了後，速やかに情報の持ち帰りを確認するとともに，記録媒体のデータはすべて削除させること。

（校務処理等における留意点）

第２８条　総括責任者等は，教職員が校務等，生徒等に閲覧されてはいけない情報を取り扱う端末等について，ユーザＩＤ及びパスワードによる管理をしなければならない。

２　教職員は，生徒等が利用するネットワークでは，生徒等に閲覧されてはいけない情報を取り扱ってはならない。

第４章　雑則

（情報セキュリティ事故等への対応）

第２９条　情報セキュリティ事故等発生時の対応については，次の点に留意しなければならない。

（１）情報漏えい・紛失・盗難・ウイルス感染等の情報セキュリティ事故が発生もしくはそのおそれがある場合は，速やかに総括責任者等に報告する。

（２）管理者は，情報セキュリティ事故の被害・影響を最小限に抑えるため，最大限の措置を講じる。

（３）管理者は，推進員等と連携し，情報セキュリティ事故の確認を行い，原因・影響範囲等を調査し記録し，総括責任者に報告する。

（４）管理者は，必要に応じ，ネットワーク管理者や警察等の関係機関に連絡するとともに連携を図る。

（５）管理者は，必要に応じ，保護者に連絡をとるとともに，生徒への適切な対応と指導を行う。

（６）管理者は，外部からの問い合わせへの対応を行う。

（７）情報化推進委員会においては，同様な事故の再発を防ぐために，具体的な対策を講じる。

（遵守状況の調査及び指導等）

第３０条　総括責任者等は，このポリシー及び実施手順の遵守状況を定期的に確認し，検査結果を記録するとともに遵守されていない事項については速やかに必要な措置を講じなければならない。

（違反行為等への対応）

第３１条　総括責任者等は，このポリシーに規定する事項又は総括責任者等の指示に違反する行為を行った教職員がある場合は，当該教職員のネットワーク及び情報機器等の利用を停止することができる。

（その他）

第３２条　このポリシーに定めるものの他，教育の情報化，ネットワーク及び情報機器等の利用に係る運用管理並びに情報セキュリティ対策に関して必要なものは，総括責任者が別に定める。

附則

（施行期日）

１　このポリシーは，令和元年１１月１日から施行する。

（様式１）

個人所有端末等利用申請書

総括責任者	管理者		推進員
校長	副校長	事務部長	

申 請 年 月 日	令和　　年　　月　　日
申 請 者 職 氏 名	㊞

申請端末等

① 端末等名称		
②使用目的		(許可)
④校内生徒用ネットワークへの接続	要　・　不要	

① 端末等名称		
② 使用目的		(許可)
④校内生徒用ネットワークへの接続	要　・　不要	

① 端末等名称		
②使用目的		(許可)
③ 校内生徒用ネットワークへの接続	要　・　不要	

（様式２）

ソフトウェアインストール申請書

総括責任者	管理者		推進員
校長	副校長	事務部長	

申　請　年　月　日	令和　　年　　月　　日
申 請 者 職 氏 名	㊞

申請ソフトウェア

①ソフトウェア名称		
②発売元もしくは開発者		
③有料・無料の種別	有料　・　無料	（許可）
④使用目的		

①ソフトウェア名称		
②発売元もしくは開発者		
③有料・無料の種別	有料　・　無料	（許可）
④使用目的		

①ソフトウェア名称		
②発売元もしくは開発者		
③有料・無料の種別	有料　・　無料	（許可）
④使用目的		

（様式３）

情報資産又はパソコン持ち出し申請書

情報資産は電子データに限る

職・氏名	申請年月日	種別 （どちらかに〇）	持ち出し理由	返却予定日	許可年月日	許可印	返却 確認日
	年　月　日	情報資産　・　パソコン		月　日	年　月　日		
	年　月　日	情報資産　・　パソコン		月　日	年　月　日		
	年　月　日	情報資産　・　パソコン		月　日	年　月　日		
	年　月　日	情報資産　・　パソコン		月　日	年　月　日		
	年　月　日	情報資産　・　パソコン		月　日	年　月　日		
	年　月　日	情報資産　・　パソコン		月　日	年　月　日		
	年　月　日	情報資産　・　パソコン		月　日	年　月　日		
	年　月　日	情報資産　・　パソコン		月　日	年　月　日		
	年　月　日	情報資産　・　パソコン		月　日	年　月　日		
	年　月　日	情報資産　・　パソコン		月　日	年　月　日		
	年　月　日	情報資産　・　パソコン		月　日	年　月　日		
	年　月　日	情報資産　・　パソコン		月　日	年　月　日		