# 個人情報保護マニュアル

会津若松ザベリオ学園中学高等学校
個人情報保護委員会

2005 年４月１日から、「個人情報保護法」が、完全施行されました。ザベリオ学園中学高等学校でも本校でも個人情報保護に関する様々な取り組みを実施し、「個人情報保護に関する規程」等の整備を進めています。しかし、トラブルの大多数は、紛失・盗難・ログオフ忘れといった、個人情報を扱う際の単純なミスや名簿等に関するずさんな管理が原因で起きています。

そこで本校では、具体的な場面を想定した教職員向けハンドブック『個人情報保護マニュアル』を作成することにしました。この冊子は「基本編」と「デジタル編」に分かれていますが、両編ともに、有効に利用されることを願います。

さて、「個人情報保護」にとって大切なことは、各個人情報に対する正確な「リスク意識」を、教職員が共有することといえます。情報を意図的に漏洩した場合は、刑事罰（懲役刑）の対象となりますが、過失であっても「個人情報」を流出させた場合は、民事上「損害賠償請求」等の対象となり、その額は莫大な金額に及びます。

個人情報保護に関する研修や訓練の重要性に加え、事案が発生したときの緊急対応も大切です。この『個人情報保護マニュアル』を熟読いただき、参考にしてほしいと思います。

2013 年４月１日

＜目 次＞

■基本編■
（１）個人情報保護管理者 ……3
（２）情報収集時の守るべき事項 ……4
（３）入室制限、施錠、保管場所 ……4
（４）ネットワーク利用時の遵守事項 ……6
（５）取扱者の限定、複製等の制限 ……8
（６）個人機器持込、情報搬出の原則 ……9
（７）保有個人情報の第三者への提供 ……10
（８）業務委託時の取り決 ……10
（９）個人情報取扱記録、保管期間、廃棄手順 ……11
（10）情報開示への対応 ……12
（11）緊急時対応、事案の報告 ……12
（12）教職員の一般的遵守事項 ……13

■デジタル編■
（13）サーバの管理 ……16
（14）コンピュータ端末の管理 ……14
（15）データの管理 ……17
（16）パスワードの管理 ……19
（17）コンピュータウィルス対策 ……19
（18）個人機器・媒体持込のルール ……20
（19）メール・Web のルール ……21
（20）用語の解説 ……22
「個人情報保護規程（案）」 ……24



〈基本編〉

**（１）個人情報保護管理者**

個人情報保護に関し、本校に次の担当者を置きます。

【個人情報保護統括管理者】 校 長

学園の総括保護管理者の下、管理責任者として、本校の保有個人情報を適切に管理する。

【個人情報保護管理責任者】 教頭（情報管理担当）、図書館情報部長

保護管理者を補佐し、本校の保有個人情報の管理に関する事務を担当する。

【個人情報保護委員会】校長　事務長　教頭及び取り扱い責任者

本校の個人情報保護等、情報管理に関する重要事項を検討する委員会。

【取扱い責任者】 企画運営委員　総務部長　図書館情報教育部長

保健環境部長など校務分掌部長、学年主任、養護教諭等　その他個人情報保護委員会が必要と認めた者

個人情報を取扱う際の直接責任者。

＜関連法規、規程、内規＞

「個人情報保護規程」（学内規程）

### （２）情報収集時の守るべき事項

個人情報を収集する際には、次のことを守る必要があります。

【利用目的の明確化、通知、公表】

利用目的を明記し、当該者に通知することが必要です。また、問い合わせ先を記しておくことが大切です。

例）「アンケート」等で、情報を収集する場合

・このアンケート（調査）は、○○○○のために利用します。回答者の住所・氏名などの個人情報は、本校からの案内等の発送（緊急連絡）のために使用し、目的外に利用することはありません。

・アンケートで収集した個人情報は、（厳重に管理します。また、本人の同意を得ることなく、）第三者に開示・提供することはありません。

＜本アンケート（調査）に対する問い合わせ先＞

会津若松ザベリオ学園中学高等学校

Tel　0242-27-1970

【利用目的に関係しない情報は収集しない】

「緊急連絡網」→ TEL．のみで対応でき、郵便物等を利用しないのなら、現住所、〒番号等は必要ありません。「念」のためとか、「とりあえず」といった発想を捨てて、絞り込んで下さい。

### （３）入室制限、施錠、保管場所等

個人情報は、重要な「資産」です。情報保管場所への勝手な出入りを許すことは、個人情報保護にとって非常に危険なことといえます。

【校舎内への入退出】



校舎内への入退出に際しては、以下のルールを設けています。

・教員以外の来校者には、以下の事項を記入してもらう。
①氏名（所属） ②入退出時刻 ③来校目的

・荷物の受け渡しに際しては、事務室前を原則とするが、状況によっては、教職員立ち会いのもと必要な場所に搬送してもらう。

【鍵管理】

個人情報保護に限らず、鍵の管理は極めて重要なことです。

・セットキーについては、総務・事務のみが保管する。

・休日出勤等で、セットキーが必要な場合は、総務・事務の了承を得た上で、「鍵管理台帳」に記載すること。

・校舎内の各部屋等の鍵を借りる場合は、事務長の了承を得た上で、「鍵管理台帳」に記載すること。

・どんな緊急時でも生徒に解錠・施錠を任せないこと。

【生徒・保護者等の入室禁止について】

個人情報にふれる機会が多いため、次の部屋への生徒・保護者の入室を禁止します。入室禁止でない部屋の場合も、入室にあたっては必ず関係者の許可が必要です。

・事務室、総務室、校長室（原則）

・印刷室、進路指導室、コンピュータ室及び準備室
※サーバルームについては、入退室記録をとる。

・理科準備室（個人情報と直接関係なし）

また、定期考査の期間中及び１週間前、成績処理期間中の教員執務室への入室は、原則禁止です。

【保管と整理整頓について】
個人情報保護のためには、各種データの整理整頓が必要です。

・重要な個人情報は、保管庫か、施錠できる引出に入れる。
・机上を整頓し、個人情報が他書類に紛れ込まないようにする。
・ファックス、プリンター、コピー機は、できるだけ取扱い責任者の目の届くところに設置する。
・ファックス、プリンター、コピー機等に個人情報に関する用紙を出力したときは、放置せず、すぐにとりに行く。
・帰宅時は、施錠及びコンピュータ、ファックス、プリンター、コピー機周辺をチェックする。

**（4）ネットワーク利用時の遵守事項**

コンピュータネットワークの利用は業務に便利な反面、「うっかりミス」や「ずさんな使用」が、莫大な個人情報の漏洩を招く危険性があります。

【パスワードとログオフ】
ネットワーク使用時における「うっかりミス」を防ぐための初歩的な確認です。

・パスワードは少なくとも６文字以上、英文字と数字、大文字と小文字を組合せるのが望ましい。氏名、生年月日、電話番号、車のナンバー等、推測されやすい文字を含むことを避ける。
・パスワードは、定期的に変更する。また、絶対他人に漏らさないこと。メモもさける。
・部屋を出るときは、必ずログオフをする。
・たとえ緊急事態であっても、教員用パソコンを生徒に使用させない。



【写真掲載時の注意】
ホームページ等に写真を掲載する時は、注意が必要です。
・個人の判定できる写真を掲載する場合は、必ず本人の許可をえる。

【メール、インターネット利用時】
メール、インターネット利用時にも度々問題が生じます。次のことを、厳守して下さい。

・インターネットやメールの私的利用は、原則禁止。
・学校宛や教職員宛に送付された公的メールを、許可なく他人のメールアドレスに送付することは禁止。
・送付対象者が限定されており、メーリングリストがある場合は、メーリングリストを利用すること。個々人のアドレスをピックアップして、送付しない。
・送信先メールアドレスのチェックを厳格にする。とくに、ＢＣＣで送付すべき所を、ＴＯやＣＣで送らない。

【インターネットを利用して個人情報を収集する場合】
公開研究会や学園祭・公開模試等の参加申込みを、インターネットを通して行うことがあります。その際の注意事項です。

①申し込みページ等の作成・管理は、情報管理委員会で行うので、ページ等を作成したい時は、必ず情報管理委員会に申しでること。
②その際、次のことを明記する。
・収集した個人情報は、他の目的に利用しない。
・個人情報はサーバで厳重に管理する。
・研究会等が終了すれば、廃棄する。

### （５）取扱者の限定、複製等の制限

書面であれ、デジタルデータであれ、保有個人情報については、取扱者を限定し、複製等を制限して、情報が不必要に拡散することを避ける必要があります。

【取扱者の限定】

- 学校の「保有個人情報」ごとに、「取扱い責任者」「取扱者」を定めるが、「取扱者」に認定されていない場合は、情報を取り扱うことができない。
- ネットワークの場合は、管理者によってアクセス制限が行われているが、書面の場合、特に気をつける必要がある。
- 連絡網、各種名簿等、教職員以外に「取扱者」が出る場合は、可能な限り対象者をしぼると共に、利用時の注意事項等を明記したうえで配布する。

【複製等の制限】

- 複製を作成するときは、可能な限り対象者をしぼると共に、重要な情報の場合は、通し番号を打った上で、誰に配付したかを記録する。
- デジタルデータをコピーする場合も同様とする。重要な情報の場合は、コピー記録（件数、利用者名）を残す。

【連絡網等配布時の注意】

各種名簿・連絡網等については、学校から持ち出して利用せざるを得ない場合も多く、利用者も教職員だけではなく、生徒・保護者に及びます。各種データによって扱いが異なります。

【教職員名簿】 教職員の氏名、住所、TEL を記載



→ 管理職に通番号を付け配布、年度末回収

【生徒名簿】生徒及び保護者の氏名、職業、住所、TEL を記載

→ 管理職、各部長・学年主任に通番号を付け配布、年度末回収

【指導カード】生徒、保護者の連絡先、住居地図等を記載

→ 担任のみ保有、コピー絶対不可

【各種連絡網】該当集団（生徒、保護者等）の TEL を記載

→ クラス、クラブ、後援会役員等該当者のみ記載し、配布。

「持出し」「保管」「使用目的」等に十分注意を払う必要があります。また、誰に配布したかを「名簿に関する台帳」に記録しておく必要があります。以下、連絡網等を配布する際の例文です。

例）「○○連絡網」につきましては、少なくとも今年度は、従来通り作成することになりました。なお、法律との関係から、以下の点ご留意下さい。

(1) この連絡網は、あくまで「○○」内、緊急連絡のためにご利用下さい。

(2) 目的外に使用したり、連絡網に記載されている Tel. 等の個人情報を第三者に漏らすことは、法律で禁止されています。

(3) この連絡網は、年度末には回収する予定ですので、厳重に保管されるようお願いします。

### （６）個人機器持込、情報搬出の原則

【個人機器持込】

私有ノートパソコン、モバイル機器等の持込自体は禁止ではありませんが、個人の情報機器をネットワークに接続し、個人情報にアクセスすることは厳禁です。

【学校機器の持出し】

学校のノートパソコン等を持出す場合は、盗難等の事態を想定し、

不必要な情報は消去した上で、「貸出記録」に記入して下さい。

【情報搬出の原則】

ここでいう「搬出」とは、紙媒体の他、ノートパソコン、USB メモリ、フロッピー等による搬出も含みます。

１．持ち出してよいが、教員が厳重保管・廃棄すべきもの。
その際、「個人情報取扱い記録（台帳）」に（持出し日時、氏名、保管場所、廃棄手続き）を記入する。
→「名簿（学校、クラス、クラブ等）」「連絡網」等

２．管理職の許可を得て、一時的に持ち出してよいもの。その際、「取扱い記録（台帳）」に（持出し日時、返却日時、氏名、保管場所）を記入する。
→「定期試験の答案」「指導カード」「推薦書」

３．持ち出せないもの。
→「指導要録」「成績一覧表」「教務手帳」「入試関係書類」

**（７）保有個人情報の第三者への提供**

原則として「保有個人情報管理規程」（学内規程）にしたがうと共に、学園（学校法人ザベリオ学園）の指導を受けながら進めます。

**（８）業務委託時の取り決め**

原則として「保有個人情報管理規程」（学内規程）にしたがうと共に、学園（学校法人ザベリオ学園）の指導を受けながら進めます。適正な業務委託先を選ぶと共に、契約書面で、以下の個人情報に関する事項について確認を交わします。また、契約期間中は、必ず契約書を保管しておく必要があります。

教務部、進路指導部、健康環境部、募集対策室など要注意です。



① 委任者及び受託者の責任の明確化、管理状況の検査に関する事項
② 委任契約範囲外の加工・利用、複写・複製の禁止
③ 個人データの漏洩防止、盗用防止及び事案の発生時の対応に関する事項
④ 委託契約期間及び契約終了後のデータの返還・消去・廃棄に関する事項
⑤ 再委託の制限または条件に関する事項
⑥ 違反した場合における契約解除の措置に関する事項

**（９）個人情報取扱記録、保管期間、廃棄手順**

【個人情報取扱い記録】

本校の保有個人情報の内容・重要度に応じて、以下の個人情報台帳等を整備し、当該個人情報の利用及び保管等の取扱い状況について、記録をとります。

① 名簿等に関する台帳
② 学籍・成績に関する台帳
③ 入試・入学に関する台帳
④ 調査書・進学資料に関する台帳
⑤ 教育実習に関する台帳
⑥ 健康診断に関する台帳
⑦ 一時的情報についての記録

また、各個人情報台帳の「取扱い記録」には、原則として次の内容を記載します。

① 取扱い責任者、取扱者 ② 使用期日、目的　　③ 利用者名 ④ 保管期間 ⑤ 搬出記録（許可情報の場合） ⑥ 更新記録 ⑦ 廃棄記録（廃棄した場合）

【廃棄時のルール等】

「ゴミ」になると価値のないものと判断しがちですが、「ゴミ箱あさり」は、古来よりスパイ活動の常套手段です。廃棄時には、個人情報を復元不可能な状態にして、廃棄することが大切です。

① 個人情報が含まれる「紙媒体」の場合、シュレッダーにかけるのが原則。シュレッダーは、事務室、中高職員室に配備してある。
② 古紙利用に際し注意が必要。個人情報の記された用紙を、不用意に再利用に回さない。
③ 重要な個人情報や大部なものを廃棄する場合は、業者に廃棄を依頼する。
④ デジタル媒体の廃棄にあたっては、メディアシュレッダーを利用するか、業者に廃棄を依頼する。
⑤ パソコンデータ及びハードディスクの廃棄については、『情報システム管理マニュアル』にしたがう。

**（10）情報開示への対応**

本校の保有個人情報の開示等の措置については、「保有個人情報開示等取扱規程」（学内規程）にしたがい、学園の個人情報保護窓口を通して行います。保有個人情報の訂正及び利用停止、異議申し立てに関することも、同様です。



**（11）緊急時対応、事案の報告**

個人情報漏洩等の問題が発生した場合は、次のような緊急対応をとります。まず、事案の発生を知った教職員はいち早く保護担当者に連絡せねばなりません。次いで、本校（校長）が事案をいち早く把握し、教職員が正しい認識を共有する必要があります。校内に「情報セキュリティー対策本部」を設置し、必要なスタッフを招集することになります。

また、事案の規模によっては、直接総括保護管理者の指令下に入ることになります。

【事案の連絡ルート】（勤務時間外、休日を含む）

発見者 → 保護担当者 → 保護管理者 → 総括保護管理者（教頭、事務長及び校長）

※必要に応じて、顧問弁護士、監督官庁、業務委託先等とも連絡をとる。

【情報危機対応時の招集順（校内の場合）】

次の通りとします。

① 校長、教頭、事務長
② 企画運営委員、情報担当教員
③ 全教職員

**（12）教職員の一般的遵守事項**

最後に、特別な個人情報を直接担当することのない、教員の一般的遵守事項について、まとめておきます。

①「情報」収集時の注意

・利用目的を明記し、当該者に通知する。また、問い合わせ先を記しておく。
・利用目的に関係しない情報は収集しない。

②「名簿」等の管理

・学校から持ち出すことは可能。ただし「名簿に関する台帳」に「取

扱い記録」を記すこと。
・自宅等で保管する場合は厳重に管理すること。「学校名簿」については、次年度当初に新名簿と交換する。他の名簿は原則としてシュレッダー等で廃棄する。
・各種連絡網は、TEL　等の最小必要限の情報掲載にとどめ、目的外使用禁止や廃棄手順について、連絡網上に掲載する。
③「学籍」等の管理
・「指導要録」等、学籍関係書類を持ち出すことは不可。
・「調査書」もデジタル化されているので、プリントアウトは必ず学校で行う。
④「成績」等の管理
・定期考査「答案」については、持ち出して採点することは可能。た
・「成績一覧表」「指導手帳」等は、書面・デジタルデータを問わず持ち出すことは不可。学校で作業すること。
⑤「保管場所」等
・各種個人情報保護に関し定めている「取扱者の限定」「入室禁止」「施錠」等の措置を厳守のこと。
・上記措置について、生徒・保護者等にも注意喚起のこと。
⑥「パソコン」使用時の留意点
・パスワードの設定は、慎重に。
・部屋を出るときは、必ずログオフをすること。
・メール発信時には、注意事項を遵守すること。
⑦「ノートパソコン・モバイル」等の持込に関して
・個人の情報機器を校内に持ち込んで、ネットワークに接続することは厳禁。
⑧「搬出」に関して
・搬出可能な個人情報については、必ず各種台帳に「搬出記録」を記入する。
・USB　メモリ、フロッピー等に個人情報をコピーして持ち出す時も同



様。
⑨ データ廃棄時の注意
・マニュアルにしたがって、情報毎に定められた方法（シュレッダー、業者委託等）で確実に廃棄する。
⑩ 事案発生時の対応
・休日であっても、いち早く保護担当者（総務・事務係長）に連絡する。
・招集がかかれば、直ちに出勤し、状況認識を共有する。

〈デジタル編〉

**（13）サーバの管理**

本校には、サーバがあり、それにデータが保存されています。重要なデータはサーバに保存して、セキュリティの確保や、各種情報の共有をはかることが大切です。

【システム管理者】

■各種サーバの管理は、システム管理者が行う。

■システム管理者は、コンピュータに詳しい教員 1 名と、図書館情報教育担当者 1 名が担当する。

■システム管理者は、サーバへのアクセスログ☆[1] を保存・管理する。

■システム管理者は、パスワードファイルを暗号化し、厳重に管理する。

■システム管理者は、年度ごとに見直す。

【アクセス制限】

■サーバへのアクセス制限は、情報管理委員会の判断に基づき、システム管理者が行う。

■アクセス制限は、年度ごとに見直す。

【管理者権限】

■システム管理者権限は、システム管理者(2 名)および総務(1 名)の 3 名に限定する。

■システム管理者権限は、年度ごとに見直す。

**（14）コンピュータ端末の管理**

教職員の利用しているコンピュータ端末が適切に管理されていないと、そこから個人情報などの重要なデータが流出してしまう恐れがあります。したがって、教職員の個々人が十分に注意して、コンピュータ端末を管理することが大切です。

【システム管理者による管理】

■システム管理者は、コンピュータ端末を台帳に登録する。



■コンピュータ端末からのログイン時には、パスワードを必要とする設定にする。

【端末利用者による管理】

■コンピュータ端末のハードディスクに、個人情報のデータを保存するのは、原則として禁止する。やむを得ず個人情報をコピーしなければならない場合は、情報管理委員会の許可を得る。

■離席、帰宅の際には、必ずログオフすること。

■帰宅の際には、コンピュータ端末の電源を落とし、ノートパソコンは施錠できる部屋で保管すること。

■コンピュータ端末には、原則として共有設定は行わないこと。

■コンピュータ端末の校外への持ち出しは、原則として禁止する。やむを得ない場合は、盗難等の事態を想定し、不必要な情報は消去した上で、情報管理委員会の許可を得て、「貸出記録」に記入して持ち出す。

■たとえ緊急事態であっても、教職員用パソコンを生徒に使用させない。

**（15）データの管理**

現代の社会では、コンピュータで様々な重要なデータを扱います。管理者も利用者も、データの管理には細心の注意を払うようにしましょう。

【データベースの管理】

■システム管理者は、データへのアクセス制限をかける。

■システム管理者は、各種データのバックアップの頻度・手順を定めて、定期的に実行する。

■バックアップを保存した記録媒体は、厳重に管理する。

■システム管理者は、システムやデータがクラッシュしたときの復旧手順を明確にしておく。

■個人情報(名簿・成績等)は、原則としてサーバーに保存し、コンピュータ端末には保存しない。

【データ運搬・記録媒体の管理】
■メール添付での個人情報の送信は、原則として禁止する。やむを得ずメール添付する場合は、暗号化やパスワードによる保護をかける。
■インターネット経由でサーバに接続する場合は、VPN☆2（Virtual Private Network）接続で行う。その場合でも、サーバの個人情報を個人のパソコンのハードディスクに保存してはならない。
■個人情報を記録媒体（USB メモリ、CD、DVD 等）にコピーするときは、情報管理委員会の許可を得ること。その場合、使用目的を達成した場合には、速やかにデータを消去すること。

■個人情報を記録媒体にコピーして校外に搬出することは、原則として禁止する。やむを得ない場合は、「個人情報取扱い記録（台帳）」に（持出し日時、氏名、保管場所、廃棄手続き）を記入し、使用目的を達成した後には、速やかにデータを消去すること。
■しかしながら、この程度の「消去」では、個人情報は簡単に復活できる。したがって、個人情報をサーバ以外のコンピュータや記録媒体にコピーするのは、可能な限り避けるべきである。

・ファイルやフォルダをごみ箱にドロップして、ごみ箱を空にしただけでは、ディスクの内容を「完全に消去」したことにはならない。
・このような操作は、本に例えれば目次を消しただけで、本文に相当する部分のデータはまだそのままディスク上に残っている。
・消去したファイルのデータに他のデータが上書きされない限りデータ復活ソフトウェアで、データを復活させることができる。
・本当にディスクの内容を消去するためには、ディスク上のすべてのセクタに渡って何らかのデータを上書きしなければならない。このような操作を行う市販のツールもある。



【データの廃棄】
■パソコンを廃棄するときは、ハードディスクを物理的に破壊するか、専用のソフトウェアでデータを上書きして完全に消去する。
■記録媒体を廃棄するときは、メディアシュレッダー等で物理的に破壊する。

**（16）パスワードの管理**
情報化社会では、パスワードは非常に重要なものです。パスワードに関する理解を深め、管理を徹底できるようにしましょう。
【パスワードの管理】
■パスワードは少なくとも 6 文字以上、英文字と数字を組合せるのが望ましい。氏名、生年月日、電話番号、車のナンバー等、推測されやすい文字を含むことを避ける。
■パスワードは、少なくとも半年に一度、定期的に変更する。また絶対、他人に漏らさないこと。メモもさける。
■パスワード入力時に、手元を見られないように注意する。
【覚えやすく安全なパスワードの作成方法】
■パスワードは、英数字だけではなく記号などを取り入れると解読されにくくなる。

**（17）コンピュータウィルス対策**
校内でコンピュータが 1 台でもコンピュータウィルス に感染すると、個人情報が流出するなど、被害は校内だけで収まらずに大変な事態となる可能性が大きいのです。十分すぎるほどの対策を講じることが大切です。
【感染予防】
■ウィルスバスターなどのウィルス対策ソフトを、サーバおよびすべてのコンピュータ端末に導入する。
■ウィルス対策ソフトが、自動的に毎日パターンファイル☆3 を更新す

る設定にしておく。
■心当たりのない添付ファイルのあるメールは、開封せずに直ちに消去する習慣をつけ、確実に消去する。
【危機管理】
■コンピュータウィルスの感染に気づいた場合は、直ちにコンピュータからLANケーブルを抜き、情報管理委員会に連絡する。
■校長は情報セキュリティー対策本部を設置し、以下の手順で危機管理にあたる。

1. 直ちに外部へのネットワークを遮断する。
2. システム管理者を中心に、感染状況の把握、感染原因の究明、ウィルスの駆除を行う。
3. 幼稚園・小学校に連絡し、必要ならば応援を要請する。

**（18）個人機器・媒体持込のルール**

私有ノートパソコン、モバイル機器等の持込自体は禁止ではありませんが、個人の情報機器をネットワークに接続し、個人情報にアクセスすることは厳禁です。
【私有ノートパソコン等の利用ルール】
■私有コンピュータを校内で端末として利用したいときは、その理由を情報管理委員会に申し出る。情報管理委員会が許可した場合は、学校に端末として固定した状態での使用を認める。
■上記で認められた場合以外は、私有コンピュータを校内ネットワークに接続すること厳禁する。
【コンピュータウィルス対策】
■個人のコンピュータおよび記録媒体を校内に持ち込む際には、必ず事前に、それらのウィルスチェックを行う。
■授業等の関係で、生徒が記録媒体を校内に持ち込む際にも、ウィルスチェックを行ってから、データのコピー等を行う。



**（19）メール・Web のルール**

メール、インターネットは、日常業務にとってなくてはならないものになりました。お互いにルールを守って、気持ちよく利用したいものです。
【メールのルール】
■メールの私的利用は、原則として禁止する。
■学校宛や教職員宛に送信された公的メールを、許可なく他人のメールアドレスに送信することは禁止する。
■自分宛てに届いたメールは、送信者が許可していない限り他人には見せない。
■自分のところへ『他の人宛のメール』が間違って届いた場合は、内容は読まずに破棄する。
■送信対象者が限定されており、メーリングリストがある場合は、メーリングリストを利用すること。個々人のアドレスをピックアップして、送付しない。
■送信先メールアドレスのチェックを厳格にする。とくに、BCC（Blind Carbon Copy）で送付すべき所を、TO や CC（Carbon Copy）で送らない。TO や CC では、ヘッダにメールアドレスが記録されるので、通常は誰が読んでいるかわかり便利であるが、場合によってはプライバシーを侵害してしまう危険性がある。
「CC」は、本来の受信者に同内容のメールが転送されたことが通知されるが、「BCC」は通知されない。
【Web のルール】
■ホームページ等に写真を掲載する時は、次のような注意が必要である。

・特定個人が判別できないように、顔などが鮮明に映らないように配慮する。また個人名を付記しない。
・個人の判定できる写真を掲載する場合は、必ず本人の許可

をえる。

■ Web を通じて、公開研究会や学園祭等の参加申し込みを受け付けるときは、次の点に注意する。

1. 申し込みページ等の作成・管理は、情報管理委員会で行うので、ページ等を作成したいときは、必ず情報管理委員会に申し出ること。
2. その際、次のことを明記する。

・収集した個人情報は、他の目的に利用しない。
・個人情報はサーバで厳重に管理する。
・研究会等が終了すれば、データは廃棄する。

（20）用語の解説

本マニュアルに現れる、なじみが薄いと思われる用語の簡単な解説です。

☆1 アクセスログ

コンピュータの利用状況やデータ通信の記録を取ること。また、その記録。操作やデータの送受信が行われた日時と、行われた操作の内容や送受信されたデータの中身などが記録される。

☆2 VPN（Virtual Private Network）

公衆回線をあたかも専用回線であるかのように利用できるサービス。インターネット上で認証技術や暗号化を用いて保護された、仮想的な専用回線を提供する。

☆3 パターンファイル

コンピュータウイルスに感染したファイルや、ネットワーク上で自己複製を繰り返すワームプログラムの特徴を収録したファイル。アンチウィルスソフト(ワクチンソフト)がコンピュータウイルスやワームを検出するのに使う。ワクチンソフト(厳密にはソフトに組み込まれたウイルス検出エンジン)ごとに、専用のパターンファイルが必要である。

# 会津若松ザベリオ学園中学高等学校
# 個人情報保護規程（案）

（目的）

第１条この規程は、ザベリオ学園中学高等学校（以下「本校」という。）が保有する個人情報の取扱いに関して必要な事項を定め、個人情報の適正な収集、管理および利用に関する本校の責務を明確にすると共に、個人の権利や利益の尊重とプライバシーの保護に資することを目的とする。

（定義）

第２条　この規程において、「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日、その他の記述等により、特定の個人が識別される、または識別され得る文書、図面、写真、フィルム、磁気テープ・磁気ディスク等の各種の媒体に記録されたもの、その他、本校が業務上取得または作成したもので、特定の個人が識別される、または識別され得るものをいう。

２　この規程において「本人」とは、現在または過去のいずれかの時点で本校と次の各号に掲げられている関係を有した者をいう。

（１） 本校の教職員およびそれに準ずる者（非常勤講師、臨時職員、派遣職員等）

（２） 本校の生徒、受講者、保護者・保証人等

（３） 本校の同窓生、ザベリオ会会員、後援会会員等

（４） 本校に入学を志願した者

３　この規程において、「個人情報の提供」とは、本校が保有する個人情報を、本校以外の機関・団体、または本人以外の個人等に渡すことをいい、複写、口頭、その他一切の伝達方法を含むものとする。

４　この規程において、「個人情報の開示」とは、本人の個人情報の内容が事実にもとづき正しく記録されているかを、本人が確認するために、その個人情報を遅滞なく本人またはその法定代理人に提示することをいう。



（責務）

第３条　本校は個人情報保護の重要性を認識し、個人の権利や利益が侵害されることのないよう、研修等の必要な措置を講じるよう努める。

（個人情報保護統括管理責任者）

第４条　本校に、個人情報保護統括管理責任者（以下「統括管理責任者」という。）を置き、校長をこれに充てる。

２　統括管理責任者は、本校全体の個人情報保護に関するすべての権限と責任を掌握し、本校における個人情報の保護に関する一切の業務を統括する。

（個人情報保護管理責任者）

第５条　統括管理責任者の下に、個人情報保護管理責任者（以下「情報管理責任者」という。）を置き、教頭をもってこれに充てる。

２　情報管理責任者は、それぞれの学校が所管する個人情報の保護に関する業務の責任を負う。

（個人情報保護委員会）

第６条　個人情報の保護を適正に行うため、会津若松ザベリオ学園中学高等学校個人情報保護委員会（以下「委員会」という。）を設ける。

２　委員会は、次の者をもって構成する。

（１） 校長、事務長、教頭

（２） 企画運営委員、総務部長、図書館情報教育部長、保健環境教育部長

（３） その他委員会が必要と認めた者

３　委員長は統括管理責任者とする。

４　委員会に副委員長をおき、図書館情報教育部長をもって充てる。

５　委員会は、次の各事項について審議する。

（１） 個人情報保護の施策に関する事項

（２） 統括管理責任者及び情報管理責任者から、個人情報の収集、利用、提供、開示及び廃棄等について付議された事項

（３） 本校が作成した個人情報保護に関する諸規程の点検に関する事項

（４） その他、個人情報の保護に関する重要事項
６　委員会は、審議にあたって必要な場合、原案作成のための小委員会または作業部会を設置することができる。
７　委員会は、審議に必要な場合、委員以外の者を出席させることができる。
８　委員会の事務は、図書館情報教育部長が行う。
（個人情報の収集）
第７条　個人情報の収集は、本校が業務を遂行する上で、必要最低限度の範囲内で行うものとす
る。
２　個人の情報の収集にあたっては、収集の目的をできるだけ具体的に明示しなければならない。
３　個人情報は、適正かつ公正な手段で収集されなければならない。
４　個人情報の収集にあたっては、収集の目的をできる限り具体的に明示した上で行うことを原則とする。ただし、次の各号のいずれかに該当するときは、この限りではない。
（１） 法令、本校の定める規程、本校が公表する個人情報保護に関する方針等、公表された資料により、個人情報を収集する目的が明らかなとき
（２） 個人の生命、身体、財産の保全上、緊急を要する場合であって、本人の同意を得ることが困難であるとき
（３） 国の機関もしくは地方公共団体またはその委託を受けた者が、法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき
（４） 出版、報道等により、すでに公にされているとき
５　本校が業務を遂行する上で、新たに蓄積する個人情報については、その目的を明らかにし、虚偽その他不正の手段により蓄積してはならない。



（個人情報の管理）
第８条　情報管理責任者は、個人情報の漏えい、改ざん、滅失または毀損を防止するため、適切な保護体制を整備しなければならない。
２　情報管理責任者は、個人情報の収集、利用、提供、保管に関する適切な規程および手続きを定め、委員会に報告しなければならない。
３　情報管理責任者は、個人情報を取り扱わせるにあたり、当該個人情報の安全管理が図られるよう、必要かつ適切な監督を行わなければならない。
４　情報管理責任者は、個人情報を保有する各部・各学年に必要に応じて情報管理主任者を置き、その権限の一部を委譲することができる。
（個人情報の利用）
第９条　個人情報の利用は、本校の業務遂行上必要不可欠な場合で、その目的をできる限り特定し、本人の同意を得て、適正に行われなければならない。
２　前項の規定にもかかわらず、次の各号のいずれかに該当するときは、本人の同意を要しない。
（１） 法令、本校の定める規程、本校が公表する個人情報保護に関する方針等、公表された資料により、個人情報を利用する目的が明らかなとき
（２） 個人の生命、身体、財産の保全上、緊急を要する場合であって、本人の同意を得ることが困難であるとき
（３） 国の機関もしくは地方公共団体またはその委託を受けた者が、法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の権利や利益およびプライバシーを不当に侵害する恐れがないと認められるとき
（４） その他、利用することについて、本校の業務遂行上必要であると委員会が認めたとき
３　他の部署が管理している個人情報を利用するときは、当該情報管理責任者あるいは情報管理主任者にその利用目的を明らかにし、書面に

よる許可を得なければならない。
４　前項の場合、利用主体、利用目的、年月日等を、別に定める書式の文書に記録し、個人情報を管理している部署、個人情報を利用する部署双方が１部ずつ保管するものとする。

（個人情報の提供）
第 10 条　個人情報の提供は、本校が業務を遂行する上で必要があると認められる場合に、提供する
個人情報の内容、目的、提供先を明示して、本人の同意を得て行うものとする。
２　情報管理責任者は、次の各号のいずれかに該当する場合に限り、本人の同意を得ることなく個人情報を提供することができる。
（１）法令の定めがあるとき
（２）個人の生命、身体、財産の保全上、緊急を要する場合であって、本人の同意を得ることが困難であるとき
（３）国の機関もしくは地方公共団体またはその委託を受けた者が、法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき
（４）その他、提供することについて、本校の業務遂行上必要であることが明らかな場合
３　前項第４号の場合、できる限り具体的に提供先および提供目的を明示しておくことを原則とする。
４　個人情報を提供する場合には、情報管理責任者は、提供先、提供目的、年月日等を文書に記録し、保管するものとする。
（個人情報の委託処理）
第 11 条　本校が、個人情報の処理等を委託するなど、個人情報を他に預託する場合は、契約等により次に列挙する内容を規定し、個人情報取扱いの基準を担保するなど適切な措置を講じなければならない。



（１）個人情報に関する秘密保持
（２）個人情報取扱いに関する安全保全
（３）再委託に関する事項
（４）個人情報取扱いに関する事故があった場合の責任配分
（５）契約終了後における個人情報の返却および消去
（個人情報の開示）
第 12 条　本校は、その保有している個人情報について、個人情報の種類、収集、目的、保有期間、情報管理主体を明らかにしなければならない。
２　情報管理責任者は、個人情報提供者またはその法定代理人から、当該本人が識別される保有個人情報の開示を請求されたときは、遅滞なく、当該保有個人情報を開示しなければならない。ただし、開示することにより、次の各号のいずれかに該当する場合には、その理由を明らかにした上で、その全部または一部について開示しないことができる。
（１）本人または第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
（２）本校の業務の適正な実施に著しい支障を及ぼすおそれがある場合
（３）法令に違反することとなる場合
３　情報管理責任者は、個人情報提供者またはその法定代理人より当該本人の個人情報に関して明らかに事実と異なる事項の訂正を請求された場合、信義に基づき誠実に対応しなければならない。
（個人情報の廃棄）
第 13 条　保有期間を過ぎた個人情報は、法令その他の規程に定めのある場合を除き、安全かつ確実な方法で速やかに廃棄しなければならない。
（個人情報のコンピュータ処理）
第 14 条　個人情報のコンピュータ処理を行うときは、入力、参照、更新、削除等の権限を明らかにすると共に、漏洩、障害、事故等に対す

る適切な安全対策を講じなければならない。
（規程の解釈）
第 15 条　この規程の運用にあたって、解釈、取扱い、適用などに疑義の生じた場合、統括管理責任者および情報管理責任者は適切な改善策を講じなければならない。

（規程違反行為に対する措置）
第 16 条　この規程が定める個人情報保護の方針に違反して、個人情報を収集、利用、提供、または毀損した者には、以下のような措置がとられる。
（１）違反者が教職員の場合：就業規則に基づく懲戒処分
（２）違反者が生徒の場合：学則に基づく懲戒処分
２　前項各号の措置と併せて、本校は違反者に対して、民事上・刑事上の法的責任を追及することができる。
（活動報告）
第 17 条　委員会は、その活動について、学長に対し、定期的に報告しなければならない。
２　重大な規程違反行為があった場合、委員会は、校長に対し、できる限り速やかに報告しなければならない。
（委任）
第 18 条　この規程に定めるもののほか、個人情報の保護に関して必要な事項は別に定める。
（規程の改廃）
第 19 条　この規程の改廃は、委員会及び企画運営委員会の議を経て職員会議が行なう。
附　則
この規程は、2013（平成 25）年７月１日から施行する。



個人情報保護マニュアル
平成 25 年 4 月 1 日　発行
会津若松ザベリオ学園中学高等学校
個人情報保護委員会
〒 965-0877　会津若松市西栄町１－１８
TEL.0242-27-1970
FAX 0242-27-3300
http://www.aizu-xavier.ed.jp/