

# 個人情報保護マニュアル

平成 31(2019)年 4 月

学校法人武田学園

# 目 次

1. 個人情報保護基本方針(ポリシー) . . . . .	1
2. 個人情報保護に関する遵守事項 . . . . .	2
3. 個人情報保護に関する情報セキュリティ対策 . . . . .	4
4. 個人情報保護に関する規程 . . . . .	12
5. 個人情報保護に関する規程実施細則 . . . . .	16
6. 個人情報保護に関する本学園の取り組みについて . . . . .	26

## 1. 個人情報保護基本方針（ポリシー）

### 個人情報保護基本方針

学校法人武田学園  
広島文教大学  
広島文教大学附属高等学校  
広島文教大学附属幼稚園

2016.4.1 改正

学校法人武田学園は、個人情報の重要性を認識し、次の取り組みを行います。

#### 1. 個人情報保護の精神

個人情報を保護することは、教育機関としての社会的責任であり、コンプライアンス（法令遵守）確保のための計画・実施と情報セキュリティの維持・向上ために継続的に努力を行います。

#### 2. 個人情報の収集と利用目的

個人情報の収集に際して、その利用目的を明確にし、適法かつ公正な手段により行います。

#### 3. 個人情報の適正な管理

個人情報の紛失、破壊、改ざん、漏えい、及び不正アクセスなどを防ぐため、取扱い基準を定めて、厳正な管理と合理的かつ最善の安全対策を講じます。

#### 4. 情報主体の権利の尊重

個人情報に関する個人の権利は最大限尊重します。個人情報の開示・訂正は、担当窓口において合理的な範囲で速やかに対応します。

#### 5. 第三者提供の制限

第三者へ情報を提供する場合は、提供先、提供内容を特定し、情報主体（本人・保護者）の同意を得て行います。それ以外の場合は、第三者に提供、開示等は法令で規定されている場合を除き、一切いたしません。

#### 6. 管理体制

全学園的な個人情報保護の取り組みを強化するために、「情報セキュリティ委員会」を設置し、個人情報を取り扱う部門ごとに管理責任者をおき、教職員の教育と啓発を継続的に実施します。

#### 7. 法令遵守

個人情報に関する法令、規範および学園内の規程を遵守します。

## 2. 個人情報保護に関する遵守事項

### (1)持ち出す場合

- ア. 次の項目を明らかにして事前に許可を得ること
  - a. 持出理由
  - b. 持出先
  - c. 持出期間
  - d. 持出情報の項目
  - e. 持出情報の件数(人数など)
  - f. 持出情報の媒体
- イ. パスワードにより保護すること
- ウ. 紙媒体を収納する時には、中身が分からないように行うこと
- エ. 盗難・紛失に注意すること

### (2)データとして送信する場合

- ア. データの送信先が学园内・学園外の如何に関わらずパスワードにより保護すること
- イ. パスワードにより保護されたファイルとそのパスワードは同一のメールでは送信しないこと
- ウ. 宛先（メールの場合には CC や BCC による送信先を含む）に間違いがないか、よく確認すること
- エ. 学園外の複数の宛先にメールにて送信する場合には、原則として、相互に宛先が分からない方法（BCC により送信 など）により送信すること

### (3)パスワードを次のように設定・管理すること

- ア. 前二項のほか、次の場合には、パスワードを設定すること
  - a. 個人情報を取り扱うパソコン、スマート端末（以下「パソコン等」という）の起動時
  - b. 個人情報を取り扱うアプリケーションソフト・Web サービスのアカウント
- イ. 数字、英小文字、英大文字、記号のうち3種類を含むこと
- ウ. 8文字以上に設定すること
- エ. 定期的に変更すること
- オ. 記録したものは、人目に付くところに記載・貼付などをしないこと
- カ. 同じパスワードの使い回しはしないこと
- キ. 他者に伝える時には、そのパスワードの入力が必要なものや ID と一緒には伝えないこと

(4)ウイルス対策を次のように実施すること

- ア. ウイルス対策ソフトをインストールすること
- イ. ウイルス対策機能は常に機能するように設定すること
- ウ. パターンファイルが最新のものに更新されるように設定すること
- エ. 定期的なウイルス検索を実行すること
- オ. USBメモリなど外部記憶媒体を使用する際にもウイルス検索を実行すること
- カ. 自宅でも職場と同様に全てのパソコン等に、上記ア～オの対策を行うこと

(5)その他の対策として次のことを実施すること

- ア. ノートパソコンやスマート端末は盗難防止対策（セキュリティーワイヤーの設置など）を実施すること
- イ. 盗難紛失が起きないように注意すること
- ウ. パソコン等を一定時間使用しない場合には、他者が使用できない（使用しようとした場合にはパスワードの入力が必要とする など）ように設定すること
- エ. 廃棄時には復元不可能なように消去できるソフトを使用して消去するか、または物理的な破壊を行うこと
- オ. OSやアプリケーションのアップデートを定期的に行うこと
- カ. ハードディスク故障による個人情報の消失に備えバックアップを定期的を実施すること
- キ. バックアップデータの紛失・盗難・漏えいの防止対策も原本データと同様に行うこと
- ク. 自宅でも職場と同様に個人情報の紛失・盗難・漏えいの防止対策を行うこと

(6)その他留意事項

- ア. 学園の法人情報・機密情報も個人情報と同様とする
- イ. 漏えいのおそれを認識した場合には、直ちに個人情報管理責任者へ報告すること
- ウ. 総括情報管理責任者は、パソコン等に対する教職員による個人情報漏えいのおそれのある操作について、そのログを収集すること

### 3. 個人情報保護に関する情報セキュリティ対策

情報に対する脅威が増大しています。特に故意に行われる行為の愉快犯的なものから、専門的な犯罪集団によるものが増加しています。

防災、自分のミス、犯罪等への防御のため、情報セキュリティへの認識をもって、個人情報流出やその他のトラブルに対応してください。また、「個人情報保護管理体制（個人情報管理者の責任と権限）」(9 ページ)及び「情報セキュリティ管理体制（情報セキュリティ管理者の責任と権限）」(10 ページ)に従って、各自の責任を果たしてください。

#### (1) 物理的対策

書類、機器などの無断持ち出しや盗難に備えて、保管庫への収納やパソコン自体に盗難に対するガードを施す必要があります。特にノートパソコンは簡単に持ち運びが出来るので、ワイヤーやチェーンで机などに固定しておきます。簡単に移動することに逆行しますが使わないときの方が盗難にあいやすいので不便でも固定してください。

特に重要な情報（個人情報、マイナンバーなど）を格納したパソコンは、上記の盗難対策以外にも、そのパソコンを操作する人を限定し、利用実績を記録するなど細心の注意を払ってください。また、インターネットに接続するとウイルス感染などの脅威にさらされることとなりますので、スタンドアローンで利用してください。

物理的よりも心がけの問題ですが、重要な情報を格納したノートパソコン、情報端末（タブレット端末、スマートフォンなど）や、記録媒体、あるいは書類などを車内の目立つ場所に放置するのはたいへん危険です。目に触れにくい場所へ置くように心がけ、場合によっては身に付けて持ち歩くことも考えてください。

デスクトップや外付けの記録媒体（ハードディスク、CD-R、DVD、その他メモリーなど）についても盗難や紛失に注意してください。

#### (2) 廃棄時の注意事項

ハードディスクなどはパソコン上でファイルの削除を行っても、復活ソフトを使うと復元されます。過去に個人情報などを記録した記録メディアは完全消去用の専用ソフトを使うか、物理的な破壊をしましょう。

破壊するときはケガをしないように注意して行ってください。

ICT 推進課では、廃棄するパソコンを定期的に回収し、専門業者にハードディスクの破壊と廃棄を委託しています。不要になったパソコンの廃棄については、ICT 推進課に連絡して指示に従ってください。

### (3) ウイルス対策

学園内で利用するパソコンは、ネットワークに接続するしないにかかわらず、学園から指定されたウイルス対策ソフトをインストールしなければなりません。新たなパソコンを学園内で利用する前に、ウイルス対策ソフトのインストールを ICT 推進課に依頼してください。

また、学内のネットワークに接続されていないと最新のウイルスの情報（パターンファイル）が取得できませんが、パソコンを起動して、学内のネットワークに接続してから、数分程度で最新のパターンファイルに更新されます。パターンファイルが更新されたことを確認してからパソコンの利用（メールの送受信、インターネットの利用や USB メモリーの装着など）を始めるようにしてください。ネットワーク以外（フロッピー、USB メモリーなど）からでもウイルス感染することがあるので注意してください。

公の機関や有名企業の名前をかたって、ウイルス付きのメールを送り付ける事例が多々報告されています。不審に感じたメールについては、決して添付ファイルを開かないで、早急に ICT 推進課まで連絡して指示を仰いでください。

もしウイルスに感染したら、パソコンの修理、全ファイルの喪失（デジカメ写真なども）、メールを授受した相手への被害など損失が甚大になることが予想されます。それらを守るためにも、パソコンの動きが普段と何だか違うなどの異状に気が付いたら、早急に ICT 推進課に連絡してください。

### (4) ファイアウォール

外部からの侵入を防御するために回線の出入り口に設置しています。今のところ突破されていませんが、絶対はありません。侵入する側と守る側の競争になります。学園でも分刻みで世界中から挑戦（アタック・攻撃）を受けています。侵入されると、学園のホームページや重要な情報を好き勝手に改ざんしたり、学園のネットワーク機器やパソコンを中継（踏み台）して他のサイトに攻撃を仕掛けます。

最近、ウイルス付きのファイルをメールで送り付け、そのファイルを開くとウイルスが活動を始め、その組織のネットワーク機器やパソコンを踏み台にするように設定を変えたり、内部の情報を外に向けて送信したりする手口が横行しています。

### (5) アップデート

ウィンドウズを始めとする OS やアプリケーションにセキュリティホール（ソフトの欠陥）があると、そこを突いてウイルスや不正プログラムが侵入してきます。

定期的にアップデートを行うことでウイルスや不正プログラムの侵入を防ぐことができます。

## (6) バックアップ

パソコンが故障した場合にバックアップが取っていないとすべてのデータを失う危険があります。また、データを誤って消去してしまうこともあるかもしれません。これらの際にデータの消失を最低限に抑えるために、データのコピーを定期的に取りっておいてください。

なお、火災に対しては、バックアップデータを離れた場所に保管しておく必要があります。

## (7) 暗号化

インターネット上やメディア上でデータを暗号化して、万が一の紛失やデータ漏えいに備える必要があります。

マイクロソフト社の Word や Excel などのオフィスソフトには、読み取りパスワードを設定することができます。読み取りパスワードを設定すると、ファイルの内容が暗号化されます。これ以外にも、暗号化ソフト、暗号化機能付き圧縮ソフトを利用することでファイルの暗号化が実現できます。

次のような場合は必ず暗号化してください。

- ① 重要な情報をメールに添付する場合には、そのメールの送信先が学园内・学園外の如何に関わらず、添付するファイルを必ず暗号化し、送信先を慎重に確認してから送信してください。なお、復号するためのパスワードは同じメールに記載せずに、別メールで送ってください。
- ② 重要な情報を USB メモリーや CD-ROM などに記録して学外へ持ち出す場合には、記録するファイルは必ず暗号化して、紛失・盗難に備えてください。

暗号化の際に設定するパスワードの強度が低い（短い・単純・容易に推測可能 など）と、パスワードを突き止められ、暗号化した情報が解読される恐れがあります。十分な強度を持ったパスワードを設定してください。ただし、設定したパスワードを忘れてしまうと自分自身でも解読できなくなります。紛失したり、詐取されたりしないような安全な方法でパスワードを管理してください。

## (8) 個人所有パソコン

自宅でも学園で行っている対策を取らないと非常に危険です。

個人情報を持ち帰っての仕事禁止する理由がここに 있습니다。自宅では、個人情報を扱う仕事は原則として禁止します。

個人所有のパソコンでも、必ずウイルス対策ソフトをインストールしてください。ウイルス対策ソフトは複数年契約のものが大半を占めていますが、契約更新を忘れないようにしてください。契約更新を忘れると新しく出現したウイルスを検知しません。



ファイル交換ソフトを利用することは、著作権を侵害している可能性が高く、違法行為として訴えられる可能性もあります。また、交換するファイルにウイルスを仕込んだりする悪意を持った人たちも利用しています。うっかりウイルスに感染させられると、パソコンの中の情報がインターネットに流出する危険があり、このようなファイル交換ソフトの利用は禁止します。ご家族で共有しているパソコンでは、家族の誰かがファイル交換ソフトを使っていないか、特に注意が必要です（家族の誰か一人でも同じパソコンでファイル交換ソフトを使っていると、情報流出の危険があります）。

(9) 個人情報の学外への持ち出し

個人情報の学外への持ち出しは原則として、禁止します。

どうしても学外へ個人情報を持ち出して仕事をしなければならない場合には、上長に「学外で仕事をしなければならない理由」、「持ち出す情報の種類、数量」、「学外で行う仕事の内容」を伝え、許可を得てください。また、その仕事が終わったら、速やかに持ち出したパソコンや USB メモリーから個人情報を消去し、上長に仕事の終了と情報の消去を行った旨を報告してください。

(10) パソコン以外の情報端末（タブレット端末、スマートフォンなど）の利用上の注意

タブレット端末やスマートフォンを利用する際には次のことに気を付けて利用してください。

- ① 不特定多数の人が出入りする場所では、原則として、上記の情報端末を使って重要な情報を扱わないでください。
- ② 上記の情報端末には、容易に他人が使えないようにパスコード、あるいはパスワードを設定してください。
- ③ 上記の情報端末を使用しているときには画面に注意が集中するため、周囲への注意が散漫になりがちです。

不特定多数の人が集まる場所や、電車・バスの中では、背後からや隣の席から覗き見されないように注意してください。

- ④ 学内メールの受信を設定している上記の情報端末には、別途お知らせする MDM（Mobile Device Management）ソフトを盗難・紛失対策のためにインストールしてください。

このソフトをインストールすることで、万が一盗難に遭ったり、紛失したりしても遠隔操作で情報端末内の情報を消去することができます。盗難に遭ったり、紛失したりした際には一刻も早く、ICT 推進課まで連絡してください。

#### (11) パソコンなどの操作ログの取得・保存

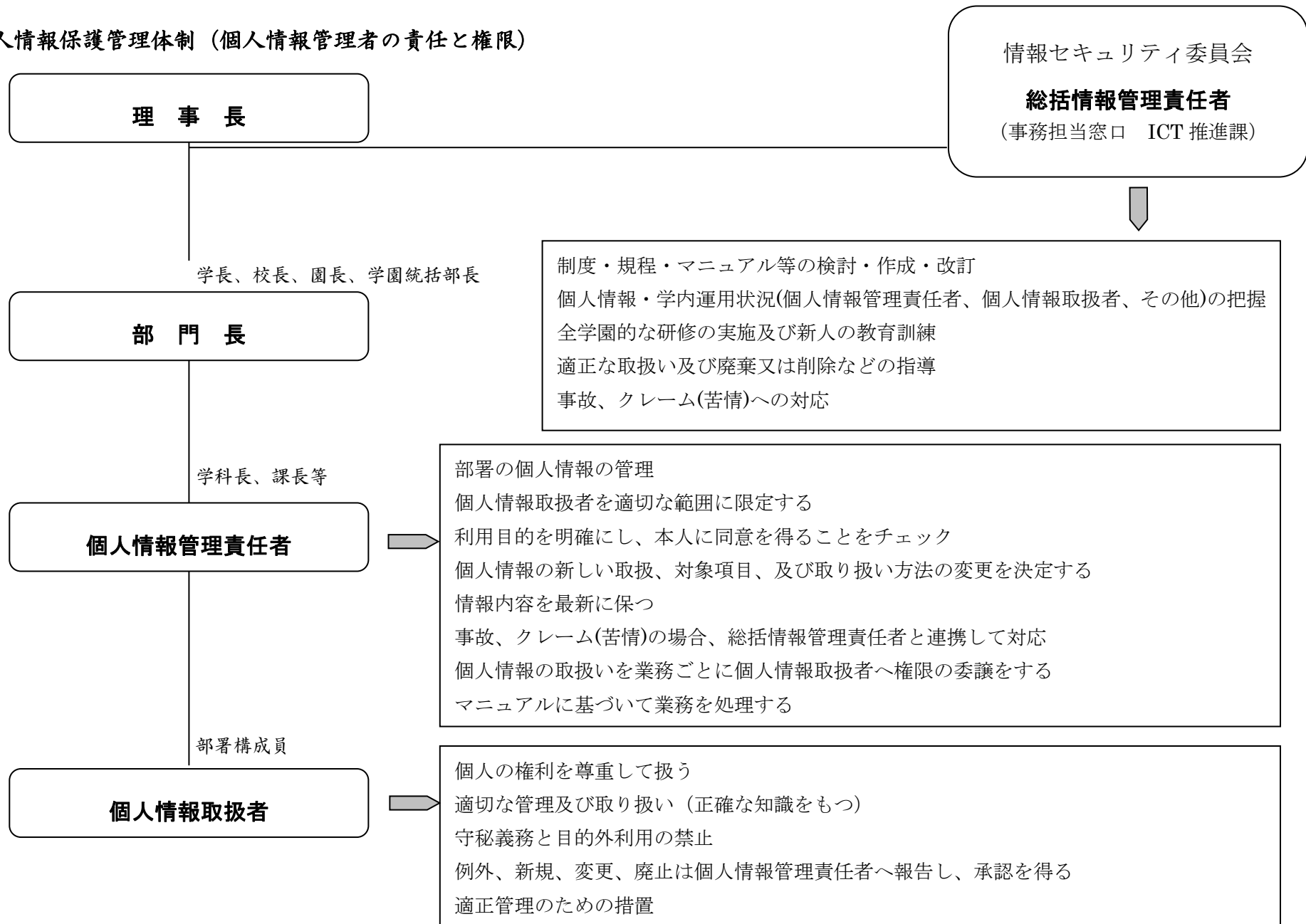
「本学ネットワーク概念図と情報持ち出し防止対策」(11 ページ)で示すように、学内からの情報流出を引き起こす可能性が高い行為があります。

- ① 学内のファイルサーバーからアクセス権を与えられていない情報を読み取る。  
→ 本来、その情報にアクセスする権限がないのに、ユーザーID、パスワードを推測、あるいは他人のユーザーID、パスワードを使ってアクセスしその内容を読み取る行為です。
- ② メール添付ファイルで学外へ送信する。  
→ 学内に限定された情報を学外へ上長の許可を得ずに送信する行為です。
- ③ 学内でオンラインストレージへ書き込み、学外で読み取る。
- ④ 外部記録媒体に書き込んで学外へ持ち出す。  
→ ③、④は、書き込み先が違うだけで、情報の持ち出しに変わりはありません。しかも、大量の情報を持ち出すことになります。
- ⑤ 印刷した紙を学外へ持ち出す。  
→ 一度に持ち出せる情報量は、上記③、④に比べると、さほど多くはありませんが、他の資料など見分けが付きにくいという特徴があります。

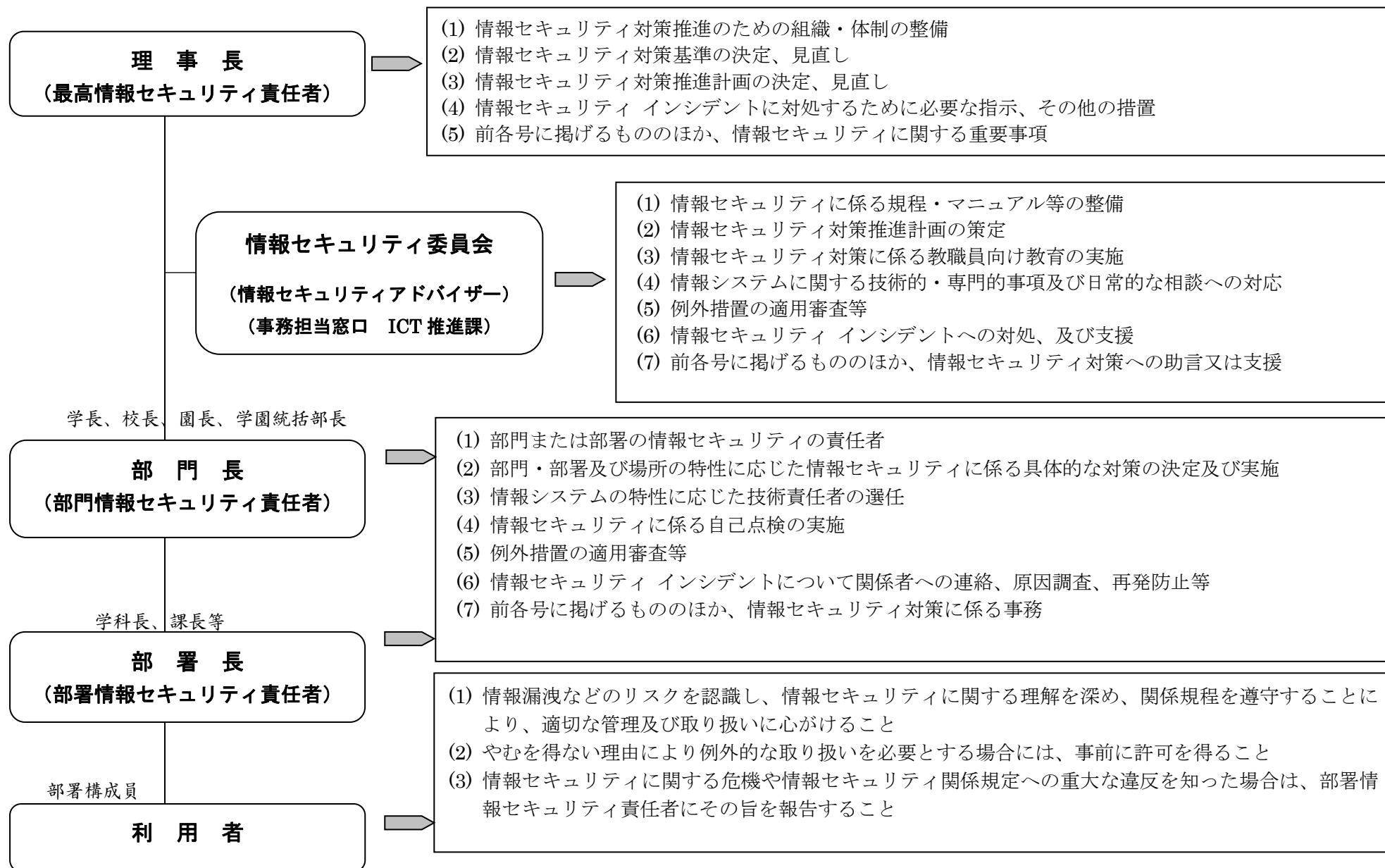
上記の①～⑤の行為について、「いつ」、「だれが」、「何を」、「どうした」について、操作ログとして取得・保存します。これにより、情報の持ち出しの発生を把握し、上長の許可を得ているか否かを確認します。

また、①については、情報へのアクセス権限を厳守するよう、システム的な対応も実施してゆきます。

個人情報保護管理体制（個人情報管理者の責任と権限）



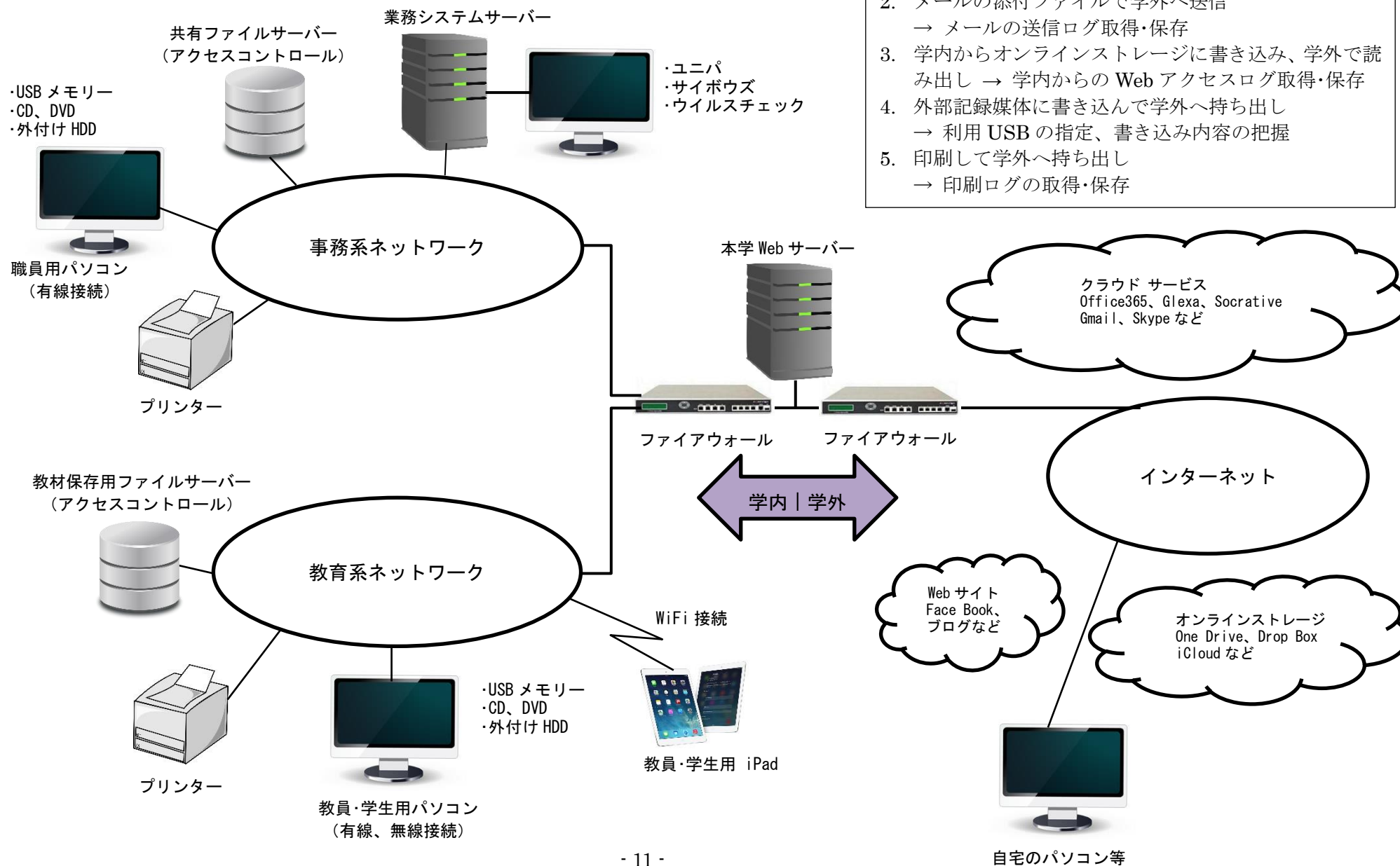
## 情報セキュリティ管理体制（情報セキュリティ管理者の責任と権限）



## 本学ネットワーク概念図と情報持ち出し防止対策

### 持ち出しリスクと防止対策（ログ取得以外に禁止・制限も含む）

1. ファイルサーバーからの読み込み  
→ ファイルサーバーへのアクセスログ取得・保存
2. メールの添付ファイルで学外へ送信  
→ メールの送信ログ取得・保存
3. 学内からオンラインストレージに書き込み、学外で読み出し → 学内からの Web アクセスログ取得・保存
4. 外部記録媒体に書き込んで学外へ持ち出し  
→ 利用 USB の指定、書き込み内容の把握
5. 印刷して学外へ持ち出し  
→ 印刷ログの取得・保存



## 4. 個人情報保護に関する規程

### 学校法人武田学園個人情報保護に関する規程

(目的)

第1条 この規程は、学校法人武田学園（以下「本学園」という。）の業務上の必要に応じて収集及び保管する個人情報の取り扱いに関する基本的な事項を定め、もって個人情報を適正に保護・管理することを目的とする。

(個人の定義)

第2条 この規程において「個人」とは、現在及び過去において、本学園の役員、本学園と雇用関係にあった教育系職員及び事務系職員（以下「職員」という。）並びに本学園の学生、生徒、園児とこれらの者の保護者等本学園の業務と係わりがあり、又は、係わりがあったすべての者をいう。

(個人情報の定義)

第3条 この規程において「個人情報」とは、本学園が業務の必要に応じて収集又は作成した次の各号に規定するものをいう。

- (1) 個人が識別される氏名、年齢、生年月日、顔写真、住所及び経歴並びに学業成績及び就職先等個人に属するすべての情報
- (2) 前号の個人に属する情報の一部又は全部が識別されるもので、記録媒体の別（文書、図画、写真、フィルム及び電子的・磁氣的に記録されたもの）によらず、すべての情報

(個人情報の守秘義務等)

第4条 職員又は職員であった者は、業務上知り得た個人情報を第三者に漏えい又は不当な目的に利用してはならない。

(管理体制)

第5条 本学園の個人情報の管理に関する事務を総括させるため、総括情報管理責任者を置き、情報セキュリティ委員会委員長をもって充てる。

- 2 各学科、各教科又は各課等（以下「部署」という。）の所管する個人情報を適正に保護するため、それぞれの部署ごとに個人情報管理責任者を置き、部署の長をもって充てる。なお、部署の長をもって充てることが適当でない場合は、別途個別に総括情報管理責任者が指名するものとする。
- 3 個人情報を管理し、又は、取り扱う役員及び職員を個人情報取扱者とする。個人情報取扱者は、職務上作成し、又は、取得した個人情報を適切に管理し、取り扱わなければならない。
- 4 個人情報取扱者は、業務上の目的以外の目的で個人情報を取り扱ってはならない。また、命ぜられた範囲以外の個人情報を取り扱ってはならない。
- 5 個人情報管理責任者は、個人情報取扱者である者を、業務の性格上などから、それぞれの業務について適切な範囲内に限定するものとする。

(個人情報の収集等の制限等)

第6条 個人情報の収集にあたっては、思想、信条及び宗教等個人の内心の自由に関する事項並びに私的生活の自由と個人の人権を侵害するおそれがあると認められる個人情報は収集し、又は、記録してはならない。ただし、業務遂行上必要不可欠な場合はこの限りではない。

- 2 前項ただし書きに定める「業務遂行上必要不可欠な場合」とは、別に定める。

(個人情報収集の原則)

第7条 個人情報は、利用目的を明確にし、本人の同意を得て、かつ、本人から収集することを原則とする。

ただし、次の各号の一に該当する場合は、本人以外の者及びその他各種機関等から収集することができる。

- (1) 本人の同意があるとき。
- (2) 法令又は本学園の規程等によって収集するとき。
- (3) 個人の生命若しくは財産の保全又は個人の安全等のために緊急の措置を要するとき。

(教育研修)

第8条 総括情報管理責任者は、個人情報の秘匿性等その重要性に鑑み、その取り扱いについて個人情報管理責任者及び個人情報取扱者に対し、適宜研修を行うものとする。

(個人情報の記録及び報告)

第9条 個人情報管理責任者は、個人情報の秘匿性等その内容に応じて、台帳等を整理して、当該個人情報の利用及び保管等の取り扱いの状況について記録するとともに、総括情報管理責任者へ適宜報告するものとする。

2 報告及び台帳等の詳細については、別に定める。

(個人情報の適正管理)

第10条 総括情報管理責任者は、個人情報の保護と正確性を維持するため、次の各号に掲げる必要な措置を講じなければならない。

- (1) 個人情報の漏えい及び改ざんの防止
- (2) 個人情報を記録した媒体の紛失、き損及び破壊の防止
- (3) 個人情報の正確性及び最新性の維持
- (4) 業務上不要となった個人情報の速やかな廃棄又は削除
- (5) その他個人情報の保護のために必要で適正な措置については、別に定める。

(個人情報の機械処理の機能の限定)

第11条 個人情報をコンピューター等によって機械処理する場合は、業務上必要最小限の範囲にその機能を限定しなければならない。

(個人情報の外部への提供等)

第12条 本学園が保管する個人情報は、次の各号の場合を除いて、本人の同意なしに本学園以外の機関、団体又は本人以外の個人等に提供してはならない。

- (1) 法令に基づく官公庁等から依頼等があったとき。
- (2) 前号の他、個人の生命又は財産の保全若しくは個人の安全等のために緊急の措置を要するとき。

2 前項による個人情報の提供にあたっては、必要最小限の個人情報とし、その目的及び提供先を明らかにして、原則として事前に個人情報管理責任者の了解を求めなければならない。

(個人情報の保管等に関する内部監査)

第13条 理事長は、個人情報の機械処理をはじめ個人情報の保管等に関する業務について、その適切性を確保するために、内部監査人を置き、適宜監査を命じることができる。

2 前項の監査については、別に定める。

(個人情報の閲覧の請求)

第14条 この規程に基づく個人は、自己の個人情報に限って、その閲覧を、該当する個人情報を保管する、個人情報管理責任者に請求することができる。

(閲覧の制限)

第15条 前条にかかわらず、閲覧目的が、個人の選考、評価等、本人に知らせないことが明らかに正当である場合は、個人情報管理責任者は、その個人情報の全部又は一部の閲覧を認めないことができる。

2 前項の場合、可能な限り、その内容等について、公表するものとする。

(個人情報の訂正の請求)

第16条 第14条による閲覧の結果、明らかに個人情報に誤りがある場合、又は、通常必要とする個人情報の記載漏れがあった場合、若しくは、第6条に違反する記載があった場合は、当該個人情報を管理する個人情報管理責任者に対して、訂正又は追加若しくは削除（以下、三者を総称する場合は「訂正等」という。）を請求することができる。ただし、本学園が必要とする個人情報の項目の削除又は業務上不要な個人情報の追加を請求することはできない。

2 前項の訂正等に当っては、その正当な理由を明示した文書をもって、個人情報管理責任者に請求しなければならない。

3 個人情報管理責任者は、前項に基づいて個人情報の訂正等を行う場合は、その事実を証明する文書等の提供を求めることができる。

(訂正等事項の関連部署への連絡)

第17条 前条に基づいて、個人情報の訂正等を行った個人情報管理責任者は、その旨を機械処理を行っている部署及びその他関連部署の個人情報管理責任者に対して、速やかに、報告しなければならない。

2 前項により報告を受けた当該個人情報管理責任者は、速やかに、機械処理による訂正を行うものとする。

(業務委託の場合の約定)

第18条 本学園以外の業者等に業務を委託する場合（学園内において処理する場合を含む。）は、個人情報の保護に必要な事項について、約定しなければならない。

2 前項により業務を委託する場合は、事前に約定書の写しを総括情報管理責任者へ提出するものとする。

(個人情報管理責任者の権限を超える問題発生の報告等)

第19条 個人情報の閲覧等をはじめこの規程の運用に伴って、個人情報に関する取り扱いに関して、個人情報管理責任者の権限では対応が不可能な問題が生じた場合、あるいは、個人情報が漏えいした場合又は、個人情報が漏えいしたおそれがある場合には、個人情報管理責任者は、速やかに、その事実及び問題の所在等を記載した文書をもって、理事長に報告しなければならない。

(問題に対する決定等)

第20条 理事長は、前条の報告があった場合、常任理事会の議を経て、問題に対する対処方法を決定しなければならない。

2 理事長は、前項の決定に当たり、常任理事会構成員以外の個人情報の保護に関する学園内外の専門家の出席を求め、その意見を聴くことができる。

(苦情の処理)



第21条 個人情報保護に関し、発生する苦情その他諸問題については、すべて ICT 推進課で受付を行うものとする。

2 ICT 推進課は、受付を行った苦情等について、総括情報管理責任者の指示を得て、関連部署の個人情報管理責任者等と協議を行い、速やかに処理を行うと共に、理事長へ報告するものとする。なお、総括情報管理責任者の判断を越えると思われる事項については、速やかに、解決のための意見を付して理事長へ報告し、その指示を得て処理を行うものとする。

3 前項の「関連部署の個人情報管理責任者等との協議」には、「情報セキュリティ委員会への付託」を含むものとする。

4 第2項中の「その指示」には、第20条に規定する「常任理事会の議を経て」を含むものとする。  
(本規程の運用に伴う細則の制定)

第22条 本規程の運用に伴う事務処理のための書式及び事務処理手続等必要な事項は、実施細則で別に定める。

(規程改正の事務処理等)

第23条 この規程改正の事務処理等については、学園統括部 ICT 推進課で行う。その他、それぞれの部署に係る事項は、それぞれの部署で処理するものとする。

2 この規程の改正は、常任理事会の審議を経た後、理事長の決裁を経て行うものとする。

附 則

この規程は、平成 17 年 8 月 26 日から施行する。

附 則

この規程は、平成 18 年 5 月 19 日から施行する。

附 則

この規程は、平成 19 年 8 月 24 日から施行する。

附 則

この規程は、平成 21 年 4 月 1 日から施行する。

附 則

この規程は、平成 22 年 4 月 1 日から施行する。

附 則

この規程は、平成 28 年 4 月 1 日から施行する。ただし、第23条第2項は平成 28 年 10 月 1 日から施行する。

## 5. 個人情報保護に関する規程実施細則

### 学校法人武田学園個人情報保護に関する規程実施細則

(目的)

第1条 この細則は、学校法人武田学園個人情報保護に関する規程（以下「規程」という。）第22条の規定により、規程の運用に関し、必要な事項について定めることを目的とする。

(個人情報管理責任者の指名)

第2条 規程第5条第2項にいう、総括情報管理責任者が指名する場合とは、様式1号にその命免を記録することにより、行うことをいう。

(個人情報の収集等の制限等の除外)

第3条 規程第6条のただし書きにいう「業務遂行上必要不可欠な場合」とは、次の各号に規定するものをいう。

- (1) 広島文教大学心理教育相談センター及び学生相談室の相談業務
- (2) 広島文教大学キャリアセンター・就職課の就職相談業務
- (3) 広島文教大学附属高等学校の学級担任、生徒指導部教員、養護教諭及びカウンセラーが行う生徒指導・相談の業務
- (4) 広島文教大学附属幼稚園の養護教諭及びカウンセラーが園児の保護者に行う園児の生活及び育児に関する指導・相談の業務

(利用目的の明示)

第4条 規程第7条に規定する「個人情報は、利用目的を明確にし」とは、帳票により収集する場合には、その帳票様式に、その旨個々に印字しておくものとする。ただし、本学園の教職員を対象とするものについては、別に定める。

(個人情報の記録及び報告)

第5条 規程第9条に規定する個人情報台帳は、様式2号とし、常時その状況を記録するとともに、個人情報管理責任者が管理・保管するものとする。

2 規程第9条に規定する報告は、次により様式3号で行うものとする。

- (1) 新たな種類の個人情報を取り扱うとき
- (2) 取扱内容に変更があるとき
- (3) 個人情報取扱者を変更するとき
- (4) その他、総括情報管理責任者の指示があったとき

(個人情報の適正管理のための措置)

第6条 規程第10条に規定する個人情報の適正管理のための措置とは、次に定めるとおりとする。

- (1) 個人情報が記録された記録媒体の別（文書、図画、写真、フィルム及び電子的・磁気的に記録されたもの）によらず、あらゆる記録媒体の学園外への移動の禁止
- (2) 個人情報の記録されたパソコン（私有物を含む。）の学園外への移動の禁止
- (3) 個人情報の送信、送付、電信等の手段による学園外への移送の禁止
- (4) 使用済みの個人情報の廃棄、消去、返却等の確認と記録あるいは、報告
- (5) 次項に定める個人情報漏えい防止対策の実施

2 前項第5号により定める個人情報漏えい防止対策は、次の各号のとおりとする。

- (1)パスワードを次のように設定・管理すること
- イ 次の場合には、パスワードを設定すること
    - i 個人情報を取り扱うパソコン、スマート端末（以下「パソコン等」という）の起動時
    - ii 個人情報を取り扱うアプリケーションソフト・Web サイトのアカウント
    - iii 個人情報を学園外へ移動（持出しなど）するとき
    - iv 個人情報を学園外へ移送（送信など）するとき
  - ロ 数字、英小文字、英大文字、記号のうち3種類を含むこと
  - ハ 8文字以上に設定すること
  - ニ 定期的に変更すること
  - ホ 記録したものは、人目に付くところに記載・貼付などをしないこと
  - ヘ 同じパスワードの使い回しはしないこと
  - ト 他者に伝える時には、そのパスワードの入力が必要なものやIDと一緒に伝えないこと
- (2)ウイルス対策を次のように実施すること
- イ ウイルス対策ソフトをインストールすること
  - ロ ウイルス対策機能は常に機能するように設定すること
  - ハ パターンファイルが最新のものに更新されるように設定すること
  - ニ 定期的なウイルス検索を実行すること
  - ホ USBメモリなど外部記憶媒体を使用する際にもウイルス検索を実行すること
  - ヘ 自宅でも職場と同様に全てのパソコン等に、イ～ホの対策を行うこと
- (3)個人情報が記録された媒体（紙資料、パソコン、スマート端末、ハードディスク、USBメモリなど）には盗難防止対策（セキュリティーワイヤーの設置や鍵のかかる保管庫に保管など）を実施すること
- (4)盗難紛失が起きないように注意すること
- (5)パソコン等を一定時間使用しない場合には、他者が使用できない（使用しようとした場合にはパスワードの入力が必要となる など）ように設定すること
- (6)廃棄時には復元不可能なように消去できるソフトを使用して消去するか、または物理的な破壊を行うこと
- (7)OSやアプリケーションのアップデートを定期的に行うこと
- (8)ハードディスク故障による個人情報の消失に備えバックアップを定期的の実施すること
- (9)バックアップデータの紛失・盗難・漏えいの防止対策も原本データと同様に行うこと
- (10)自宅でも職場と同様に個人情報の紛失・盗難・漏えいの防止対策を行うこと
- (11)漏えいのおそれを認識した場合には、直ちに個人情報管理責任者へ報告すること
- (12)総括情報管理責任者は、パソコン等に対する教職員による個人情報漏えいのおそれのある操作について、そのログを収集すること
- 3 第1項第1号から第3号の規定は、次の各号のいずれにも該当する場合は、適用しないものとする。
- なお、いずれの場合にあっても必要最小限のデータに厳選し、かつ、慎重に処理するものとする。
- (1) 学生，生徒，園児及び職員にかかる諸申請手続並びに事業等学園の業務（所属の長が認めたもの）遂行のとき

- (2) 本人の同意を得たとき
  - (3) 所管部署で所定の使用許可を得たとき
  - (4) 前項に定める個人情報漏えい防止対策を適切に実施するとき
- 4 前項第3号の使用許可は、様式第7号により次の各号の項目を明らかにして事前に行うものとし、業務終了後、速やかに、第1項第4号の手続等処理を完了し、その旨記録保存するものとする。
- (1)持出理由
  - (2)持出先
  - (3)持出期間
  - (4)持出情報の項目(住所、氏名など)
  - (5)持出情報の件数(人数など)
  - (6)持出情報の媒体
- 5 第3項の規定により個人情報を学園外へ持ち出す場合には、次の各号の個人情報漏えい防止対策を実施すること。
- (1)パスワードにより保護すること
  - (2)紙媒体を収納する時には、中身が分からないように行うこと
  - (3)盗難・紛失に注意すること
- 6 第3項の規定により個人情報をデータとして送信する場合には、そのデータの送信先が学園内・学園外の如何に関わらず、次の各号の個人情報漏えい防止対策を実施すること。
- (1)パスワードにより保護すること
  - (2)パスワードにより保護されたファイルとそのパスワードは同一のメールでは送信しないこと
  - (3)宛先（メールの場合にはCCやBCCによる送信先を含む）に間違いがないか、よく確認すること
  - (4)学園外の複数の宛先にメールにて送信する場合には、原則として、相互に宛先が分からない方法（BCCにより送信 など）により送信すること
- 7 学園の法人情報・機密情報もその重要性に鑑み、個人情報と同様に漏えい防止対策を実施すること。

(個人情報の外部への提供の場合の報告)

第7条 規程第12条第2項に規定する個人情報の外部への提供等を行う場合の報告は、様式4号により行うものとする。

(内部監査)

第8条 規程第13条に規定する内部監査は、次のとおり行うものとする。

- 2 内部監査は、必要に応じて実施するものとする。
- 3 内部監査は、聞き取り調査を主とし、必要に応じて、帳票等関係書類の提示を求めるものとする。
- 4 内部監査の結果、改善を要する事項の指摘があった場合は、監査人は、理事長に報告するとともに、当該部署に対して、文書で通知するものとする。

(個人情報の閲覧の請求)

第9条 規程第14条に規定する閲覧の申し出は、様式5号により行うものとする。

- 2 前項の場合に、経費を要したときには、実費相当額（当分の間、複写経費は、1枚10円とする。）を徴収するものとする。

(個人情報の訂正の請求)

第10条 規程第16条に規定する訂正の申し出は、様式5号により行うものとする。

(業務委託の場合の約定)

第11条 規程第18条に規定する個人情報の保護に必要な事項として約定に定める事項は、次に定める事項とする。

- (1) 個人情報保護法による守秘義務の遵守について
- (2) 提供する個人情報の範囲
- (3) 業務委託の期間
- (4) 業務場所、業務従事者の状況、監督者、業務責任者
- (5) 提供した個人情報の使用の内容
- (6) 委託業務終了後のデータの返却或いは、処分方法
- (7) 再委託の場合の詳細
- (8) 事故発生の場合の報告
- (9) その他、データ複製の制限等留意事項

(問題発生の場合の報告等)

第12条 規程第19条に規定する問題発生の際は、速やかに、様式6号により、理事長へ報告するとともに、被害の拡大防止の措置を行うものとする。

附 則

この細則は、平成17年8月26日から施行する。

附 則

この細則は、平成18年5月19日から施行する。

附 則

この細則は、平成18年6月30日から施行する。

附 則

この細則は、平成19年4月2日から施行する。

附 則

この細則は、平成19年8月24日から施行する。

附 則

この細則は、平成28年12月1日から施行する。

附 則

この細則は、平成31年4月1日から施行する。

○ 様式1号 個人情報管理責任者の指名

No. \_\_\_\_\_

整理 番号	起 案 年月日	決 裁 欄			所 属 (範 囲)	氏 名	本 人 確 認	開始年月日
	決 裁 年月日	理事長	総括情報管 理責任者	ICT 推進課				終了年月日

(以下省略)

○ 様式2号 個人情報台帳(「情報資産調査票」を活用することもよい。)

No. \_\_\_\_\_

整理番号	作成年月日	情報名称	記録媒体区分	対象者	件数	個人情報項目 (記号)	個人情報 管理 責任者印
	廃棄年月日	利用目的				記入者所属・氏名	

(以下省略)

凡 例

1. 記録媒体区分: 1=帳票 2=冊子 3=FD 4=CD-ROM 5=コンピュータファイル
2. 対象者 : 1=学生、生徒、園児 2=保護者 3=入学希望者 4=卒業生  
5=司書講習受講者 6=公開講座受講者 7=教職員 8=その他
3. 個人情報項目: 1=氏名 2=生年月日 3=住所 4=電話番号 5=携帯電話  
6=メールアドレス 7=成績 8=写真 9=その他

○ 様式3号 変更報告書

平成 年 月 日

総括情報管理責任者 様

所属部署

氏 名

変 更 報 告 書

このたび次のとおり、変更があったので、個人情報保護に関する規程第9条の規定により報告いたします。

記

1. 変更の内容
2. 期 日
3. そ の 他

注)他の様式の資料を活用して添付いただくことで補完してください。

○ 様式4号 個人情報の外部への提供の場合の報告

平成 年 月 日

個人情報管理責任者 様

所属部署

氏 名

個人情報の外部への提供

このたび次のとおり、個人情報を外部へ提供したので、個人情報保護に関する規程第12条2項の規定により報告いたします。

記

1. 提 供 の 内 容  
(目的・提供先・提供する情報の範囲など)
2. 期 日
3. そ の 他



○ 様式5号 個人情報の閲覧の請求並びに個人情報の訂正の請求

平成 年 月 日

所属部署名[            ]  
個人情報管理責任者 様

所属部署  
氏 名

個人情報の閲覧[訂正]の請求

このたび次のとおり、個人情報の閲覧[訂正]をしたいので、個人情報保護に関する規程第14条[第16条]の規定により請求いたします。

記

1. 閲覧[訂正]の内容
2. 期 日
3. そ の 他

注) 目的に応じて、文中の「閲覧」及び「訂正」の用語を抹消してください。

○ 様式6号 個人情報に係る問題の発生について

平成 年 月 日

理 事 長 様

所属部署  
氏 名

個人情報に係る問題の発生について

このたび次のとおり、問題が生じたので、個人情報保護に関する規程第19条の規定により報告いたします。

記

1. 報告の内容
2. 期 日
3. そ の 他

注) 必要に応じて、関係の帳票の写しを添付してください。

## 個人情報学園外持出許可簿

部署名

No	日付	氏名	持出期間	持出先	持出情報の内容	持出理由	媒体	部署長等承認日・印	事後処理実施日・印
1	/ /		/ / ~ / /				・紙 ・USBメモリ ・パソコン ・iPad ・その他 ( )	/ / 印	/ / 印
2	/ /		/ / ~ / /				・紙 ・USBメモリ ・パソコン ・iPad ・その他 ( )	/ / 印	/ / 印
3	/ /		/ / ~ / /				・紙 ・USBメモリ ・パソコン ・iPad ・その他 ( )	/ / 印	/ / 印
4	/ /		/ / ~ / /				・紙 ・USBメモリ ・パソコン ・iPad ・その他 ( )	/ / 印	/ / 印

1. 持ち出す者が太枠内を記入
2. 太枠内について、学科長・センター長・部署長等が確認し、「部署長等承認日・印」欄に承認日を記入のし、押印する
3. 持ち出しの終了後は、適切に廃棄・消去等を実施してください。実施後には、「事後処理実施日・印」欄に実施日を記入し、押印する。

持ち出す際には、個人情報保護規程実施細則第 条に定められている個人情報の漏えい対策を実施すること

○ 様式7号(その2) 個人情報の学園外持出許可願

学科長・関係部課長 (個人情報管理責任者)

平成 年 月 日

個人情報管理責任者 様

所属・役職

氏 名

印

個人情報学園外持出許可願

この度、下記のように個人情報を学園外へ持出したいので、個人情報保護に関する規程第10条及び同規程実施細則第6条により、ご許可願います。

また、持出しの終了した個人情報は、廃棄・消去・返却等の確認と記録あるいは報告を速やかに行います。

記

- 1)持ち出す理由 \_\_\_\_\_
- 2)持出先 \_\_\_\_\_
- 3)持出期間 \_\_\_\_\_ 月 日 ~ \_\_\_\_\_ 月 日
- 4)持出情報の項目・件数 \_\_\_\_\_
- 5)持出情報の媒体 \_\_\_\_\_ 紙 ・ USBメモリ ・ パソコン ・  
iPad ・ その他 ( \_\_\_\_\_ )

学科長・関係部課長

上記の個人情報について、廃棄・消去・返却等を実施しましたので、その旨を報告します。

【方法】 廃棄 ・ 消去 ・ 返却 ・ その他 ( \_\_\_\_\_ )

【実施日】 平成 年 月 日

平成 年 月 日

所属・役職・氏名

印

※ 持ち出す情報については、個人情報の漏えい防止対策を実施のこと  
持ち出しは、個人情報管理責任者の承認を得た後に行うこと

## 6. 個人情報保護に関する本学園の取り組みについて

本学園では、学生、生徒及び園児とその保護者又は、保証人並びに教職員（以下「学生等」という。）の個人情報をデータベース化し、教育・研究及び修学支援に必要な業務を遂行するために利用しています。一方、個人の尊厳及び基本的人権の尊重の立場から、プライバシーを中心とした個人情報は、確実に保護されなければなりません。

本学園では、個人情報の保護に関する法律や政令、文部科学大臣が定める指針等の基準を尊重しながら、個人情報の保護に努めています。さらに、全学的な情報セキュリティポリシー「個人情報保護基本方針」の下で、個人情報保護に関する学園規程を制定し、個人情報の収集、管理、利用、開示、提供について技術的、組織的な対策を講じるとともに、教職員に対する全学的な教育・啓発活動を通じて個人情報の適正な利用と保護に努め、あわせて、対策、基準及び遵守状況の継続的な評価、見直しを行いながら、常に、改善を図っております。

なお、ここに記述しましたことは、本学園の業務遂行に伴い、特に、修学する学生等の教育指導のために必要なものです。

これらについて疑義がある場合は、学園統括部 ICT 推進課へお問い合わせください。

記

### 1. 個人情報の保護について

個人情報データベースを利用するにあたり、個人情報の有用性に配慮しつつ、個人の権利及び利益を保護することを目的として、「個人情報の保護に関する規程」を制定しています。その内容は、次のとおりです。

#### (1) 「個人情報」とは

現在及び過去の学生等並びに入学予定者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、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより、特定の個人を識別することができることとなるものを含む。）をいいます。

#### (2) 利用目的の特定

個人情報は、本学園における教育・研究及び学生等の修学支援に必要な業務を遂行するために利用します。

#### (3) 適正な取得

個人情報は、直接当該本人から取得するなど、適正な手段により取得します。

なお、思想、信条及び宗教に関する個人情報は、いかなる理由があろうともこれを取得しません。

#### (4) 利用目的の通知等

本人から直接書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）に記載された当該本人の個人情報を取得する場合には、あらかじめ本人に対し、その利用目的を明示します。（この書面に記載の内容を含みます。）

利用目的を変更した場合は、変更された利用目的について、本人に通知又は公表します。

(5) データ内容の正確性の確保

個人データは、利用目的の達成に必要な範囲内において、正確かつ最新の内容に保ちます。したがって、提供いただいた個人データに変更が生じた場合には、速やかにお申し出ください。

(6) 安全管理措置

個人データの漏えい、滅失又はき損の防止、その他の個人データの安全管理のために必要かつ適切な措置を講じています。教職員に学生等の個人データを取扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該教職員に対する必要かつ適切な監督を行っています。個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託した個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行っていきます。

(7) 第三者提供の制限

個人データは、あらかじめ本人の同意を得ないで第三者に提供いたしません。ただし、①法令に基づく場合、②個人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき、③その他、学長が特に必要であると認めたときは、この限りではありません。

(8) 開示

本人から当該本人が識別される個人データの開示を求められたときは、本人に対し遅滞なく当該個人データを開示します。ただし、開示しないことが相当であるときは、個人データの全部又は一部について開示しないことがあります。その際、本人に対して遅滞なく理由を付してその旨を通知します。

(9) 訂正等

本人から、当該本人が識別される個人データの内容が事実でないという理由によって、当該個人データの訂正、追加又は削除を求められたときは、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき当該個人データの訂正等を行います。

なお、個人データの内容の全部若しくは一部について訂正等を行ったとき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく理由を付してその旨（訂正等を行ったときは、その内容を含む。）を通知します。

2. 個人情報の利用目的について

個人情報は、次のとおり本学園の教育・研究及び学生等の修学支援などの必要な業務を遂行するために、利用します。なお、利用目的を変更した場合は、変更された利用目的について、本人に通知又は公表します。

(1) 学生等の個人情報

入学関係：入学志願者に対する選抜試験運営、入学手続（編入学、再入学を含む。）、学生証等身分証の交付

修学関係：履修相談・修学指導、学業奨励、研究活動支援、履修登録、教職等諸資格課程登録、授業・試験運営、成績処理・評価、単位認定、進級・卒業判定、諸資格申請・判定（認定）、学位記授与、単位互換協定による国内留学、海外留学、短期海外研修、国

際交流、教育実習、施設実習、卒業論文

学籍関係：休学・復学・退学・転学部・転学科等身分異動

学園生活：学園生活全般に関わる指導・助言、福利厚生施設の紹介、奨学生申請・選考、奨学金交付・償還、学納金、定期健康診断、日常的な健康相談、課外活動支援、弔慰、災害見舞、卒業アルバム

進路関係：キャリア（進路）形成支援、求職登録、就職斡旋、資格取得のための課外講座運営

施設利用：図書館、情報教育（パソコン）実習室、外国語教育施設・視聴覚施設、教室、体育施設、学寮運営、駐車場、合宿施設等

同窓関係：同窓会との連携、卒業生への各種連絡・アンケート調査

その他：各種連絡・通知、諸証明書発行、用具・備品等の貸与、学則による処分

## (2) 保証人等の個人情報

学生等の修学指導等に必要な連絡。各種送付物（学業成績通知書、学費納付書、行事案内等）の発送。

## (3) 教職員等の個人情報

人事・労務関係業務の処理。業績の把握。業務連絡。

## 3. 個人情報の第三者提供について

本学園では、学生等の個人情報を次のとおり第三者に提供することがあります。なお、これ以外に提供の必要が生じた際には、その都度、本人から意思確認の手続きを取ります。

### (1) 学生等の学業成績等、修学状況を保証人に提供する

本学園では、保証人（保護者等）と連携した個別修学指導を教育上有用な取り組みと考えており、成績が確定した段階で保証人宛に「学業成績通知書」を送付し、修学状況に関する問い合わせや相談等に応じております。また、大学では、各地で開催する教育懇談会において保証人（保護者等）に、学生等の単位取得状況や進級・卒業条件の充足度などを提示しながら、進学や就職、学園生活に関し、個別面談を行っております。

しかしながら、個人情報の保護に関する法律に従い、学生本人が同意しない場合には、当該学生についてのこれ等の情報提供などは行うことはいたしません。

### (2) 学生の個人情報を就職情報サービス会社に提供する

本学では、学生等の就職活動を支援するため、就職関連情報を提供する業者に対して学生等の連絡先、（本人氏名、郵便番号、住所、電話番号等）を提供することがあります。業者の選定にあたっては、サービスの有益性はもとより個人情報保護システムが確立していること（例えば、「プライバシーマーク」を取得していること）を条件としています。なお、この件に関する同意確認は、対象学年になった際に改めてご案内いたします。

(以 上)