Guidelines for Personal Information Protection

個人情報保護に関するガイドライン

November 30, 2011
平成２３年１１月３０日
Approved by Vice President for Administrative Compliance
副学長（アドミニストレイティブ・コンプライアンス担当）決定
【Partial Revision】March 1, 2015
【一部改正】平成２７年３月１日
【Partial Revision】March 23, 2016
【一部改正】平成２８年３月２３日
【Partial Revision】May 9, 2016
【一部改正】平成２８年５月９日
【Partial Revision】May 30, 2017
【一部改正】平成２９年５月３０日
【Partial Revision】April 1, 2018
【一部改正】平成３０年４月１日
Approved by Chief Operating Officer
チーフ・オペレーティング・オフィサー決定

Article 1. Purpose

第１条　目的

The purpose of these Guidelines is to set forth the handling of personal information by the Okinawa Institute of Science and Technology School Corporation (hereinafter, the "School Corporation") so as to provide for the smooth and appropriate administration of the business and operations of the School Corporation while protecting the rights and interests of the individual.

Individuals tasked with the responsibilities as detailed in these guidelines, may in some cases not have direct control of the resources required to action them. In this case the individual responsible is to work with the relevant parties, such as the CIO, whom has direct control of the resources required to ensure that the responsibilities are met. Further rules may be imposed locally by the School Corporation, these rules and may only increase the level of restrictions, but shall not decrease the level of restrictions.

このガイドラインは、学校法人沖縄科学技術大学院大学学園（以下「学園」という。）における個人情報の取扱いに関する基本的事項を定めることによ

り、学園の事務及び事業の適正かつ円滑な運営を図りつつ、個人の権利利益を保護することを目的とする。
このガイドラインで定められる各責任者は、その責務を果たすうえで必要なリソースを直接管理権していない場合には、CIOその他の管理権を有する関係者と連携をとることが求められる。学園は、追加的なルールによりこのガイドラインより更に制限を強めることはできるが、制限を緩めることはできない。

Article 2. Definitions

第２条　定義

The terms used in these guidelines shall be construed in accordance with Article 2 of the Law concerning Access to Personal Information Held by Independent Administrative Institutions (Law No. 59 of 2003; hereinafter, the "Law").
このガイドラインにおける用語の意義は、「独立行政法人等の保有する個人情報の保護に関する法律」（平成15年法律第59号。以下「法」という。）第２条の定めるところによる。

Article 3. General Manager for Personal Information Protection

第３条　個人情報総括保護管理者

1. The Chief Operating Officer (hereinafter referred to as "COO") shall be appointed as the General Manager for Personal Information Protection of the School Corporation.
学園に、個人情報総括保護管理者（以下「総括保護管理者」という。）１名を置き、チーフ・オペレーティング・オフィサー（Chief Operating Officer）（以下「COO」という。）をもって充てるものとする。
2. The General Manager for Personal Information Protection shall have general responsibility for the management of personal information retained by the School Corporation.
総括保護管理者は、学園における保有個人情報の管理に関する事務を総括するものとする。

Article 4. Personal Information Protection Manager

第４条　個人情報保護管理者

1. Each section shall appoint one Personal Information Protection Manager, which position shall be filled by the head of the section. This role will normally have overlap with the Information Asset Manager role as defined in [PRP 17.4.8], with a single individual fulfilling both roles in most cases.

各セクション等の部署に、個人情報保護管理者（以下「保護管理者」という。）１名を置き、当該セクション等の部署の長をもって充てるものとする。個人情報保護管理者は、通常、PRP17 章で規定される 情報資産管理責任者 [Link:17.4.8]と同一の者が行う。

2. The Personal Information Protection Manager shall have general responsibility for the management of personal information retained by the section. The Personal Information Protection Manager shall be responsible for ensuring appropriate management of retained personal information. When the section handles retained personal information by information system, T¥the Personal Information Protection Manager shall work with CIO ,which is determined by Article 6 of this guideline.
保護管理者は、当該セクション等の部署における保有個人情報の管理に関する事務を統括するものとする。保護管理者は、各部署における保有個人情報の適切な管理を確保する任に当たる。保有個人情報を情報システムで取り扱う場合、保護管理者は、本ガイドライン第６条に定める最高情報責任者と連携して、その任に当たる。

Article 5. Personal Information Protection Officer
第５条　個人情報保護担当者

1. The Personal Information Protection Manager from each section shall appoint one Personal Information Protection Officer to be the Document Management Officer as set forth in the PRP 12.3.4.3.2.
各セクション等の部署に、当該セクション等の部署の保護管理者が指名する個人情報保護担当者（以下「保護担当者」という。）１名を置き、PRP 12.3.4.3.2 に定める文書管理担当者をもって充てるものとする。
2. The Personal Information Protection Officer shall assist the Personal Information Protection Manager and shall be in charge of day-to-day operations relevant to the management of the personal information retained in the section.
保護担当者は、保護管理者を補佐し、各セクション等の部署における保有個人情報の管理に関する事務を担当するものとする。

Article 6. Chief Information Officer
第６条　最高情報責任者

1. The School Corporation appoints, based on PRP2.4.1.3 and 17.4.7,the Chief Information Officer (hereinafter, the “CIO”).
学園は、PRP2.4.1.3及び17.4.7の規定により、最高情報責任者（以下「CIO」という。）１名を置く。

2. CIO shall be responsible for management of information system and cyber security program. CIO shall work with General Manager for Personal Information Protection and Personal Information Protection Manager for ensuring appropriate personal information protection management by information system and for facilitating appropriate information system.
CIOは、学園の情報システムの管理及びサイバーセキュリティープログラムに関して責任を有する。CIOは、統括保護管理者や保護管理者と連携し、学園の情報システムを用いた保有個人情報の適切な管理及び適切な情報システムを整備する任に当たる。

Article 7. Chief Information Security Manager
第７条　最高情報セキュリティ責任者

1. The School Corporation appoints Chief Information Security Manager (hereinafter "CISM"), which position shall be filled by CIO appointment based on PRP 17.4.7.
学園は、最高情報セキュリティ責任者（以下「CISM」という。）1名を置き、PRP17.4.7に基づきCIOが指名する者をもって充てるものとする。
2. CISM shall be responsible for developing information security related policies and procedures, as well as conducting risk assessment and ensuring overall information security enforcement in OIST.
学園における情報セキュリティ方針、手続き及び管理技術を策定し、情報セキュリティ管理策の実効性をリスクアセスメントなどにより監督する任に当たる。

Article 8. Personal Information Protection Auditor
第８条　監査責任者

1. The auditor of the School Corporation shall be appointed as the Personal Information Protection Auditor.
学園に、個人情報保護監査責任者（以下「監査責任者」という。）を１名置くこととし、監事をもって充てるものとする。
2. The Personal Information Protection Auditor shall be responsible for auditing the status of management for retained personal information.
監査責任者は、保有個人情報の管理の状況について監査する任に当たるものとする。

Article 9. Personal Information Protection Committee
第９条　個人情報保護委員会

If the General Manager for Personal Information Protection finds it necessary, he/she shall establish a Personal Information Protection Committee, which consists of relevant staff members, to determine important matters related to the management of retained personal information and to provide relevant communication and coordination, etc. and hold the meeting periodically or as necessary.
総括保護管理者は、保有個人情報の管理に係る重要事項の決定、連絡・調整等を行うため、必要があると認めるときは、関係職員を構成員とする委員会を設け、定期に又は随時に開催するものとする。

Article 10. Staff Training
第１０条　職員研修

1. The General Manager for Personal Information Protection shall provide staff members(including temporary staff members; hereinafter the same) handling retained personal information adequate training in matters of retained personal information handling and increase general awareness of personal information protection.
総括保護管理者は、保有個人情報の取扱いに従事する職員（派遣職員を含む。以下同じ。）に対し、保有個人情報の取扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他必要な研修を行うものとする。
2. The General Manager for Personal Information Protection shall work with the CIO to ensure staff members involved in the management of information systems handling retained personal information have the necessary training in the management, operations, and security of information systems to enable appropriate management of retained personal information.
総括保護管理者は、CIO と連携し、保有個人情報を取り扱う情報システムの管理に関する事務に従事する職員に対し、保有個人情報の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な研修を行う。
3. The General Manager for Personal Information Protection shall implement training for Personal Information Protection Managers and Personal Information Protection Officers for the appropriate management of personal information in each section, etc.
総括保護管理者は、保護管理者及び保護担当者に対し、部署等の現場における保有個人情報の適切な管理のための教育研修を実施する。

Article 11. Staff Responsibilities
第１１条　職員の責務

Staff members shall adhere to the letter and intent of all relevant laws, ordinances and guidelines, etc. and follow the instructions of the General Manager for Personal Information Protection, Personal Information Protection Manager, and Personal Information Protection Officer.
職員は、法の趣旨に則り、関連する法令及び例規等の定めを遵守するとともに、総括保護管理者、保護管理者及び保護担当者の指示に従い、保有個人情報を取り扱わなければならない。

Article 12. Access

第１２条　アクセス制限

1. The Personal Information Protection Manager shall work with the CIO to restrict the staff with access to personal information and the details of that access to the minimum scope required for those staff members to implement their work, as warranted by the confidentiality and nature of the retained personal information.保護管理者は、CIO と連携し、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する職員とその権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限るものとする。
2. Unauthorized Staff members shall not access personal information.
アクセス権限を有しない職員は、保有個人情報にアクセスしてはならない。
3. Staff members shall not access personal information for non-operational purposes.
職員は、アクセス権限を有する場合であっても、業務上の目的以外の目的で保有個人情報にアクセスしてはならない。

Article 13. Personal Information Copying, Distribution, etc.

第１３条　複製等の制限

When handling personal information for operational purposes, the Personal Information Protection Manager shall limit the cases in which the actions listed below can be carried out as warranted by the confidentiality and nature of the personal information in question, and staff members shall follow the instructions of Personal Information Protection Manager relating to;:

職員が業務上の目的で保有個人情報を取り扱う場合であっても、保護管理者は、次の各号に掲げる行為については、当該保有個人情報の秘匿性等その内容に応じて、当該行為を行うことができる場合を限定し、職員は、保護管理者の指示に従わなければならない。

(1) Copying of personal information

保有個人情報の複製

(2) Distribution of personal information

保有個人情報の送信

(3) Distribution to outside parties or distribution of media containing personal information

保有個人情報が記録されている媒体の外部への送付又は持出し

(4) Other inappropriate management of personal information

その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為

Article 14. Error Amendment, etc.

第１４条　誤りの訂正等

Staff members, as instructed by the Personal Information Protection Manager, shall promptly correct personal information errors, etc.

職員は、保有個人情報の内容に誤り等を発見した場合には、保護管理者の指示に従い、訂正等を行わなければならない。

Article 15. Electronic Media, File Management

第１５条　媒体の管理等

Staff members shall store personal information media in a designated location as instructed by the Personal Information Protection Manager, and when deemed necessary, store said media under lock and key in a fireproof safe.

職員は、保護管理者の指示に従い、保有個人情報が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫への保管、施錠等を行うものとする。

Article 16. Electronic Media, File Destruction, etc.

第１６条　廃棄等

In the event that personal information files, media (including storage, terminals, and servers) is no longer needed, staff members, as instructed by the Personal Information Protection Manager, shall delete relevant information and/or destroy relevant media in a manner that renders it impossible to recover or decipher the retained personal information.

職員は、保有個人情報又は保有個人情報が記録されている媒体（端末及びサーバに内蔵されているものを含む。）が不要となった場合には、保護管理者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行わなければならない。

Article 17. Personal Information Handling Records

第１７条　保有個人情報の取扱状況の記録

As warranted by the confidentiality and nature of the personal information, the Personal Information Protection Manager shall create ledgers, etc. and record the status of personal information use, storage, and handling.

保護管理者は、保有個人情報の秘匿性等その内容に応じて、台帳等を整備して、当該保有個人情報の利用及び保管等の取扱いの状況について記録しなければならない。

Article 18. Personal Information File Ledgers Management, etc.

第１８条　個人情報ファイル簿の管理等

1. School Corporation shall prepare and publish a register Personal Information File Ledgers describing the following matters, as designated by a Cabinet Order, with regard to the respective Personal Information Files held by the School Corporation.

学園は、保有している個人情報ファイルについて、それぞれ次に掲げる事項を

記載した個人情報ファイル簿を作成し、公表しなければならない。

（１） Name of the Personal Information File
個人情報ファイルの名称

（２） Name of the said Incorporated Administrative Agencies and the name of the organizational section in charge of the affairs for which the Personal Information
学園の名称及び個人情報ファイルが利用に供される事務をつかさどる組織の名称。

（３） Purpose of Use of the Personal Information File
個人情報ファイルの利用目的

（４） Matters recorded in the Personal Information File (hereinafter referred to as the "Recorded Matters" in this article) and the scope of individuals that are recorded in the Personal Information File as Individuals Concerned (limited to those who can be identified through a search without other description about the individual including the name and date of birth; the same shall apply in item 7 of the following paragraph) (such scope shall be hereinafter referred to as the "Scope of Record" in this article)
個人情報ファイルに記録される項目（以下、「記録項目」という。）及び本人（他の個人の指名、生年月日その他の記述等によらないで検索し得る者に限る。以下、同じ。）

（５） Method of collecting the Personal Information recorded in the Personal Information File (hereinafter referred to as the "Recorded Information" in this article)
個人情報ファイルに記録される個人情報（以下、「記録情報」という。）の収集方法

（６） When Special Care-required Personal Information is included in the Recorded Information, that effect
記録情報に要配慮個人情報が含まれるときは、その旨

（７） Where the Recorded Information is routinely provided to a party outside the said Incorporated Administrative Agencies, the name of such party
記録情報を当該独立行政法人等以外の者に経常的に提供する場合には、その提供先

（８） Name and address of the organizational section that accepts the request prescribed in paragraph 1 of the next article, Article 27, paragraph 1, or Article 36, paragraph 1 of the Law
法１２条第１項、２７条第１項、又は３６条第１項の規定による請求を受理する組織の名称及び所在地

（９） Where the proviso of Article 27, paragraph 1 or the proviso of Article 36, paragraph 1 applies of the Law, a description to that effect
法第二十七条第一項ただし書又は第三十六条第一項ただし書に該当するときは、その旨

(１０)Other matters designated by a Cabinet Order
その他政令で定める事項

2. The Rules and Procedures Section shall create, store, and publish personal information file ledgers.
個人情報ファイル簿は、法令セクションが整備し、保管及び公表する。
3. The Personal Information Protection Manager shall formally request the Rules and Procedures Section when updating the personal information file ledger and, whenever necessary, amend matters recorded to the personal information file ledger.
保護管理者は、個人情報ファイル簿に記載すべき個人情報ファイルを保有したとき、又は個人情報ファイル簿に記載されている事項を訂正等する必要があるときは、個人情報ファイル簿を更新するよう法令セクションに連絡しなければならない。

Article 19. Access
第１９条　アクセス制御

1. The Personal Information Protection Manager shall work with the CIO to take necessary measures, as warranted by the confidentiality and nature of personal information (in this article, Article 24 and Article 27 through Article 31, this shall be limited to retained personal information handled in information systems), to control access by establishing security measures (passwords, smart cards, biometrics) to verify authorization (hereinafter, "Authentication Functions").
保護管理者は、CIO と連携し、保有個人情報（以下、本条から第２４条及び第２７条から第３１条において情報システムで取り扱うものに限る。）の秘匿性等その内容に応じて、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずるものとする。
2. When taking security measures described in the preceding paragraph, the Personal Information Protection Manager shall work with the CIO to initiate any rules for the management of passwords, etc. (including regular and as-necessary reviews) and take any required security measures in order to prevent the theft of passwords, etc.
保護管理者は、CIO と連携し、前項の措置を講ずる場合には、パスワード等の管理に関する定めを整備（その定期又は随時の見直しを含む。）するとともに、パスワード等の読取防止等を行うために必要な措置を講ずるものとする。

Article 20. Records Access

第２０条　アクセス記録

1. The Personal Information Protection Manager shall, as warranted by the confidentiality and nature of retained personal information, work with the CIO to enact such measures as may be necessary to record access to personal information, retain access records for a predetermined regularly audit access records.
   保護管理者は、CIO と連携し、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、及びアクセス記録を定期に分析するために必要な措置を講ずるものとする。
2. The Personal Information Protection Manager shall work with the CIO to take any necessary measures to prevent the unauthorized modification, theft, or unauthorized destruction of access records.
   保護管理者は、CIO と連携し、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講ずるものとする。

Article 21. Monitoring of Access

第２１条　アクセス状況の監視

In order to monitor inappropriate access to personal information, the Personal Information Protection Manager shall, as warranted by the confidentiality and nature of such information, work with CIO to take measures necessary to check at regular intervals.
保護管理者は、CIO と連携し保有個人情報の秘匿性等その内容に応じて、当該保有個人情報への不適切なアクセスの監視のため、定期的確認等の必要な措置を講ずる。

Article 22. Authority of Managers

第２２条　管理者権限の設定

The Personal Information Protection Manager shall, as warranted by the confidentiality and nature of personal information, take measures necessary such as to get sign in document to acknowledge that they will be subject to disciplinary action by the School Corporation if they conduct improper manipulation, in order to minimize harm in the event of theft of system administrative authority and prevent internal improper manipulation of such information, etc.
保護管理者は、保有個人情報の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に搾取された際の被害の最小化及び内部からの不正操

作等の防止のため、不正操作を行った際は学園による懲戒的な処分の対象となることに同意する書面に署名を得る等の必要な措置を講ずるものとする。

Article 23. Prevention of Unauthorized External Access

第２３条　外部からの不正アクセスの防止

The Personal Information Protection Manager shall, as warranted by the confidentiality and nature of retained personal information, work with CIO to take such measures as may be necessary to prevent unauthorized external access to IT systems handling personal information (e.g. firewall establishment to control access pathways)

.保護管理者は、CIO と連携し、保有個人情報の秘匿性等その内容に応じて、保有個人情報を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講ずるものとする。

Article 24. Prevention of Unauthorized Disclosure Prevention Due to Malware

第２４条　不正による漏えい等の防止

The Personal Information Protection Manager shall work with CIO to take　measures necessary to eliminate vulnerabilities exposed in software and prevent the infection of IT system by malware that has grasped such vulnerabilities (including maintaining introduced software in its most up to date state at all times), in other to prevent the unauthorized disclosure, loss, or damage of personal information die to　malware.

保護管理者は、CIO と連携し、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムによる保有個人情報の漏えい、滅失又は毀損の防止のため、不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずるものとする。

Article 25Processing of Personal Information in Information Systems

第２５条　情報システムにおける保有個人情報の処理

If carrying out an action such as copying personal information temporarily to process it, staff members shall limit the personal information subject to such action to the minimum necessary, and shall promptly delete any information no longer required after processing is complete.

The Personal Information Protection Manager shall, as warranted by the confidentiality and nature of the personal information in question, confirm the situation from time to time with a focus on the state of implementation of deletion, etc.

職員は、保有個人情報について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去する。

保護管理者は、当該保有個人情報の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認する。

Article 26. Encryption

第２６条　暗号化

The Personal Information Protection Manager shall, as warranted by the confidentiality and nature of retained personal information, work with CIO to take necessary security measures to encrypt personal information.

Staff members shall, as warranted by the confidentiality and nature of personal information, carry out encryption appropriately(Actions such as the selection of appropriate passwords and measures to prevent their unauthorized disclosure are included) on the personal information that they process based on these security measures.

保護管理者は、CIO と連携し、保有個人情報の秘匿性等その内容に応じて、その暗号化のために必要な措置を講ずるものとする。職員は、これを踏まえ、その処理する保有個人情報について、当該保有個人情報の秘匿性等その内容に応じて、適切に暗号化（適切なパスワードの選択、その漏えい防止の措置等を含む）を行う。

Article 27. Information Verification, etc.

第２７条　入力情報の照合等

Staff members shall verify input against original copies, as warranted by the importance of retained personal information handled by information systems, in order to confirm the content of personal information before and after processing, and verify, etc. the integrity of existing personal information.

職員は、情報システムで取り扱う保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行うものとする。

Article 28. Personal Information Backup

第２８条　バックアップ

The Personal Information Protection Manager shall, as warranted by the importance of retained personal information, take necessary security measures to create and provide decentralized storage of personal information backups.

保護管理者は、保有個人情報の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講ずるものとする。

Article 29. IT System Design Documents Management, etc.

第２９条　情報システム設計書等の管理

The Personal Information Protection Manager shall take necessary security measures to store, copy and destroy, etc. IT system design documents, schematic diagrams, and other documentation for information systems related to personal information.

保護管理者は、保有個人情報に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずるものとする。

Article 30. Personal Information Terminals

第３０条　端末の限定

The Personal Information Protection Manager shall, as warranted by the confidentiality and nature of retained personal information, take necessary security measures to restrict terminals at which retained information may be accessed.

保護管理者は、保有個人情報の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講ずるものとする。

Article 31. Terminal Theft Prevention, etc.

第３１条　端末の盗難防止等

1. The Personal Information Protection Manager shall take necessary security measures to prevent the theft and/or loss of terminals.

   保護管理者は、端末の盗難又は紛失の防止のため、必要に応じ、端末の固定、執務室の施錠等の措置を講ずるものとする。

2. Staff members shall not remove terminals from the School Corporation premises or bring in terminals from outside except when deemed necessary by the Personal Information Protection Manager.

   職員は、保護管理者が必要があると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。

Article 32. Third Party Viewing Prevention

第３２条　第三者の閲覧防止

Staff members shall take necessary security measures to prevent the viewing of personal information by third parties when terminals are used (guidelines for logging off IT systems).

職員は、端末の使用に当たっては、保有個人情報が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずるものとする。

Article 33. Restrictions on Connection of Devices and Media with Recording Functions

第３３条　記録機能を有する機器・媒体の接続制限

The Personal Information Protection Manager shall, as warranted by the confidentiality and nature of personal information, work with CIO to take measures necessary to restrict connection of smartphones, USB flash drives, and other devices and media with recording functions to information system terminals (including upgrade of such devices) in order to prevent unauthorized disclosure, loss, or damage of personal information. They shall further ensure that the system terminals are prevented from accessing inappropriate cloud or other online services to the maximum reasonable extent possible.

保護管理者は、CIO と連携し保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の漏えい、滅失又は毀損の防止のため、スマートフォン、USB メモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講じなければならない。また、システム端末からの不適切なクラウドやその他オンラインサービスへのアクセスをできる限り防止する措置を講ずるものとする。

Article 34. Access Management

第３４条　入退の管理

1. The Personal Information Protection Manager shall work with CIO to authorize persons to enter the core server room and other areas in which equipment handling personal information is located (hereinafter, the “Server Room, etc.”) and take necessary security measures to confirm purpose of entry, log room access, identity, ensure that staff members are present when outsiders are granted access . or that such outsiders are monitored by monitoring systems, and restrict or inspect the bringing in, use, and taking out of external electromagnetic media. If other media storage contains personal information, similar measures shall be taken when deemed necessary.

   保護管理者は、CIO と連携し、保有個人情報を取り扱う基幹的なサーバ等の機器を設置する室その他の区域（以下「電子計算機室等」という。）に立入る権

限を有する者を定めるとともに、用件の確認、入退の記録、部外者についての識別化、部外者が立ち入る場合の職員の立会い又は監視設備による監視、外部電磁的記録媒体等の持ち込み、利用及び持ち出しの制限又は検査の措置を講ずるものとする。また、保有個人情報を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、同様の措置を講ずるものとする。

2. The Personal Information Protection Manager shall, when deemed necessary, work with CIO to simplify the management of server room access by identifying Server Room, etc. entrances and exits and restricting location signs.
保護管理者は、CIO と連携し、必要があると認めるときは、電子計算機室等の出入口の特定化による入退の管理の容易化、所在表示の制限等の措置を講ずるものとする。
3. The Personal Information Protection Manager shall work with CIO to enact security measures to manage access to the Server Room, etc. and storage facilities (installing access Authentication Functions and formulating rules for the management of passwords, etc.; including regular and as-necessary reviews) and take such measures as to prevent the theft of passwords, etc.
保護管理者は、CIO と連携し電子計算機室等及び保管施設の入退室の管理について、必要があると認めるときは、立入りに係る認証機能を設定し、及びパスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずるものとする。

Article 35. Server Room, etc. Management

第３５条　電子計算機室等の管理

1. The Personal Information Protection Manager work with CIO to shall take security measures as may be necessary to prevent unauthorized intrusions (providing locks, alarms, and monitoring equipment for the Server Room, etc.)
保護管理者は、CIO と連携し、外部からの不正な侵入に備え、電子計算機室等に施錠装置、警報装置、監視設備の設置等の措置を講ずるものとする。
2. The Personal Information Protection Manager shall work with CIO to take preventative measures against natural disaster, etc. by providing the Server Room, etc. with anti-seismic, fireproofing, smoke proofing and waterproofing equipment, ensuring reserve power supplies for servers/other equipment and prevent damage to wiring.
保護管理者は、CIO と連携し、災害等に備え、電子計算機室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講ずるものとする。

Article 36. Personal Information Provisions

第３６条　保有個人情報の提供

1. When providing personal information to outside parties other than administrative agencies and independent administrative institutions pursuant to Article 9, Paragraph 2, subparagraphs 3 and 4 of the Law, the Personal Information Protection Manager shall document the party receiving information by specifying the purpose of use, the legal rationale for the work in which used, the scope and content of usage records and the form of use, etc.

   保護管理者は、法第９条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について書面を取り交わすものとする。

2. When providing personal information to outside parties other than administrative agencies and independent administrative institutions pursuant to Article 9, Paragraph 2, subparagraphs 3 and 4 of the Law, the Personal Information Protection Manager shall require the enactment of security measures and shall, when deemed necessary, perform on-site inspections prior to provision and periodically thereafter to confirm the status of measures, record findings and seek improvements, etc.

   保護管理者は、法第９条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求等の措置を講ずるものとする。

3. When providing personal information to administrative agencies and independent administrative institutions pursuant to Article 9, Paragraph 2, Subparagraph 3 of the Law, the Personal Information Protection Manager shall, when deemed necessary, take the measures as set forth in the preceding two paragraphs.

   保護管理者は、法第９条第２項第３号の規定に基づき行政機関又は独立行政法人等に保有個人情報を提供する場合において、必要があると認めるときは、前二項に規定する措置を講ずるものとする。

Article 37. Operations Outsourcing, etc.

第３７条　業務の委託等

1. When outsourcing operations related to the handling of retained personal information, all necessary security measures shall be taken to avoid selection of parties lacking the capacity to appropriately manage personal information. Contracts shall specify the matters listed in items (1) to (6) below and document the contractor's and operators'

management and operational systems, provisions relating to inspection of personal information management practices, and any other necessary matters.

保有個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置を講じなければならない。また、契約書に、次に掲げる事項を明記するとともに、委託先における責任者及び業務従事者の管理及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認するものとする。

(1) Obligations to protect the confidentiality of personal information and prohibit it from being used for any purpose other than that intended 個人情報に関する秘密保持、目的外利用の禁止等の義務

(2) Restrictions on subcontracting or conditions for subcontracting, such as a requirement to seek prior approval
再委託の制限又は事前承認等再委託に係る条件に関する事項

(3) Restrictions on copying, etc. of personal information
個人情報の複製等の制限に関する事項

(4) Response to unauthorized disclosure or other incident involving personal information
個人情報の漏えい等の事案の発生時における対応に関する事項

(5) Destruction of personal information and return of digital media at the conclusion of outsourcing
委託終了時における個人情報の消去及び媒体の返却に関する事項

(6) Contract cancellation procedures , liability for damages, and other necessary measures in the event of breach of contract
違反した場合における契約解除、損害賠償責任その他必要な事項の措置その他必要な事項

2. When outsourcing operations related to the handling of retained personal information, as warranted by the confidentiality and nature of the relevant personal information, the contractor's personal information management practices shall be checked through regular inspections conducted at least annually.
保有個人情報の取扱いに係る業務を外部に委託する場合には、委託する保有個人情報の秘匿性等その内容に応じて、委託先における個人情報の管理の状況について、年１回以上の定期的検査等により確認する。

3. If a contractor sub-contracts operations involving the handling of personal information, the contractor shall be required to take the measures described in Paragraph1 above and, as warranted by the confidentiality and nature of the relevant personal information, the measures described in Paragraph 2 above shall be taken

either via the contractor or directly by the party outsourcing the operations. The same requirements shall apply if operations involving the handling of personal information are further sub-contracted.
委託先において、保有個人情報の取扱いに係る業務が再委託される場合には、委託先に１の措置を講じさせるとともに、再委託される業務に係る保有個人情報の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが２の措置を実施する。保有個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。

4. When temporary staffs handle personal information, temporary staff referral contracts shall contain explicit provisions regarding the confidentiality obligations and other aspects of the handling of personal information.
保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記しなければならない。

Article 38. Incident Reporting, Recurrence Prevention Measures, etc.
第３８条　事案の報告及び再発防止措置

1. In the event of unauthorized disclosure, other incidents that pose security problems for personal information, or the possibility of occurrence of a problem, the staff member who became aware of the matter　shall report right away before confirming the facts, which takes time to the Personal Information Protection Manager and Personal Information Protection Officer responsible for the management of the personal information.
保有個人情報の漏えい等安全確保の上で問題となる事案が又は問題となる事案の発生のおそれを認識した場合に、その事案等を認識した職員は、時間を要する事実確認を行う前に、直ちに当該保有個人情報を管理する保護管理者及び保護担当者に報告する。

2. The Personal Information Protection Manager shall take the necessary measures right away to prevent the expansion of damage and incident recovery. However, measures that can be taken right away to prevent the expansion of damage such as disconnecting the LAN cables of terminals that are suspected to have undergone unauthorized access from an external source or infection by malware shall be taken right away (including making staff members take them).
保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、外部からの不正アクセスや不正プログラム感染が疑われる当該端末等の LAN ケーブルを抜くなど、被害拡大防止のため直ちに行い得る措置については、直ちに行う（職員に行わせることを含む。）ものとする。

3. The Personal Information Protection Manager shall identify the chain-of-events leading to the incident and the extent of damage, etc. and shall report in a timely manner to the General Manager for Personal Information Protection. However, incidents deemed particularly serious shall be immediately reported to the General Manager for Personal Information Protection.
保護管理者は、事案の発生した経緯、被害状況等を把握し、速やかに総括保護管理者に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に当該事案の内容等について報告する。
4. Upon receiving reports pursuant to the preceding paragraphs, the General Manager for Personal Information Protection shall report the nature, history and damage, etc. of the incident to the President and in a timely manner as warranted by the nature of the incident.
総括保護管理者は、前項に基づく報告を受けた場合には、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を理事長に速やかに報告する。
5. The General Manager for Personal Information Protection shall promptly provide information to the Okinawa Development and Promotion Bureau of the Cabinet Office in question with regard to the details of the incident, its background and the state of damage received in accordance with the facts of the incident.
括保護管理者は、事案の内容等に応じて、事案の内容、経緯、被害状況等について、内閣府（沖縄振興局）に対し、速やかに情報提供を行う。
6. The Personal Information Protection Manager shall analyze the factors resulting in the incident and shall take such measures to prevent further recurrence.
保護管理者は、事案の発生した原因を分析し、再発防止のために必要な措置を講じなければならない。

Article 39. Public Announcement, etc.

第３９条　公表等

The President shall, as warranted by the nature and impact, etc. of the incident, publicly announce the facts of the incident and measures to prevent recurrence, and determine responses(such as communication with the people related to the personal information that was disclosed without authorization.), etc. to persons whose personal information was involved in the incident.

Information shall be provided promptly to the Ministry of Internal Affairs and Communications (Administrative Management Bureau) with regard to the facts of an incident that is to be announced publicly, the background to it and the damage received.

理事長が必要を認めるときは、事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への対応（漏えい等が生じた保有個人情報に係る本人への連絡）等の措置を講ずるものとする。公表を行う事案については、当該事案の内容、経緯、被害状況等について、速やかに総務省（行政管理局）に情報提供を行うものとする。

Article 40. Inspection

第４０条　点検

The Personal Information Protection Manager shall inspect on a regular and as-necessary basis the digital recording media, processing channels and storage methods, etc. for personal information in his or her section and shall report findings to the General Manager for Personal Information Protection.

保護管理者は、各部署等における保有個人情報の記録媒体、処理経路、保管方法等について、定期に及び必要に応じ随時に点検を行い、必要があると認めるときは、その結果を総括保護管理者に報告するものとする。

Article 41. Audit

第４１条　監査

The Personal Information Protection Auditor shall perform regular and as-necessary audits　(including independent audits by external auditors; hereinafter the same)of the management at the School Corporation in question, including the state of the measures stipulated in Article3 to Article36, to verify the appropriate management of of personal information, and shall report the findings to the General Manager for Personal Information Protection.

監査責任者は、保有個人情報の管理の適切な管理を検証するため、3 条から 39 条に規定する措置の状況を含む学園における保有個人情報の状況について、定期に及び必要に応じ随時に監査（外部監査を含む。以下同じ。）を行い、その結果を総括保護管理者に報告する。

Article 42. Evaluation and Review

第４２条　評価及び見直し

The General Manager for Personal Information Protection and the Personal Information Protection Manager shall evaluate measures for the appropriate management of personal information from the perspective of their effectiveness on the basis of audit or inspection findings and shall review such measures when deemed necessary.総括保護管理者、保護管理者等は、点検又は監査の結果等を踏まえ、実効性等の観点から保有個人情報

の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講ずるものとする。

Article 43. Cooperation with Government Agencies

第４３条　行政機関との連携

The School Corporation shall carry out appropriate management of the personal information in its possession in close cooperation with the Okinawa Development and Promotion Bureau of the Cabinet Office in question based on Paragraph 4 of the "Basic Policy on the Protection of Personal Information" (Cabinet Decision, April 2, 2004).

学園は、「個人情報の保護に関する基本方針」（平成 16 年 4 月 2 日閣議決定）4 を踏まえ、内閣府（沖縄振興局）と緊密に連携して、その保有する個人情報の適切な管理を行う。

Article 44　Other Provisions

第４４条　細則等の定め

1. Necessary matters related to the clerical processing of and fees for requests for disclosure, requests for amendment and requests for suspension of use, etc. shall be specified separately.
   開示請求、訂正請求、利用停止請求等の事務処理及び手数料等に関し必要な事項は、別に定める。
2. In addition to these Guidelines and the provisions set forth in the preceding paragraph, the COO shall formulate necessary matters for the clerical processing of personal information.
   本ガイドライン及び前項に規定する定めのほか、個人情報保護の事務処理に必要な事項は、COO が定めるものとする。