Rules for the Handling of Personal Information at Tokyo International University Foundation

Revised June 28, 2024

Chapter 1　General Provisions

Article 1:　Purpose

1. The purpose of these Rules is to ensure the proper handling of personal information and facilitate appropriate and smooth-running operations at the Tokyo International University Foundation (hereinafter the “Foundation,” including Tokyo International University, the Japanese Language School Affiliated with Tokyo International University, and Hitotsubashi Gakuin Preparatory School (hereinafter the “Schools” collectively or “Each School” respectively) while helping to protect the rights and interests of individuals by providing the guidelines necessary for proper handling of personal information retained by the Foundation, based on the Act on the Protection of Personal Information (Act No. 57 of 2003, hereinafter the “Protection Act”).

2. Matters regarding the protection of personal information which are not provided in these Rules shall be as provided in the Protection Act and the Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003) and other relevant laws and regulations (hereinafter “Personal Information Laws, etc.” which includes the Protection Act).

3. Handling of Individual Numbers (“My Number”) and specific personal information shall be as stipulated in the Rules for the Handling of Individual Numbers and Specific Personal Information at Tokyo International University Foundation[Arc trans1].

Article 2:　Policy on the Protection of Personal Information

Based on a deep understanding of the importance of protecting personal information, in the course of its efforts to protect personal information the Foundation shall formulate a policy on the protection of personal information and make the policy widely available on its official website and other media.

Article 3:　Definitions

Within these Rules, the meanings of the following terms shall be as defined as follows in each respective term.

(1)　Personal information: Information pertaining to students and their guarantors, as well as officers, faculty and staff members, alumni, and other individuals affiliated with the Foundation or the Schools, within which specific individuals can be identified from the names, birthdates, individual identification codes, and other entries or descriptions included

(including that which can readily be checked against other information to identify specific individuals).

(2) Applicable Person(s): Specific individual(s) identified from Personal Information.

(3) Individual Identification Codes: Characters, numbers, symbols, and other codes that identify some characteristics of any specific individual which have been converted via computer and can either identify that specific individual, or characters, numbers, symbols, and other codes that have been separately allotted to specific individuals and can identify those individuals.

(4) Sensitive Personal Information: Personal information which includes race, beliefs, social status, medical history, criminal history, having been victim of crime, and other entries or descriptions which must be handled with particular care so that individuals are not subjected to unjust discrimination, prejudice, or other disadvantageous treatment.

(5) Personal Information Databases, etc.: Collection of Personal Information which have been systematically compiled so that specific Personal Information can be searched by computer, or such collection of Personal Information systematically compiled according to a certain rule so that specific Personal Information can readily be searched by sorting.

(6) Personal Data: The Personal Information that populates Personal Information Databases, etc.

(7) Retained Personal Data: Personal Data which the Foundation has authorization to disclose, to correct, add to, or delete content, suspend usage, delete, and suspend provision to third parties.

Article 4: Responsibilities

The Foundation may take the following measures to fulfill the purposes stipulated in Article 1.

(1) Inform the Applicable Person(s) of the policy on the protection of personal information.

(2) Thoroughly ensure that officers, faculty and staff members, and others at the Schools and the Foundation comply with personal information protection-related laws and regulations, the policy on the protection of personal information, and related rules and regulations.

(3) Conduct activities to raise awareness of personal information protection among officers, foundation employees, and others at the Schools and the Foundation.

Article 5: Persons Responsible for Managing Personal Information

1. The Foundation shall protect personal information smoothly in an appropriate manner, and

shall appoint each respective person responsible for managing personal information (hereinafter “Person Responsible”) as follows in order to clarify where that responsibility lies.

(1) Person Responsible for Overall Management of Personal Information (hereinafter “Person Responsible for Overall Management”)

(2) Person Responsible for Departmental Management of Personal Information (hereinafter “Person Responsible for Departmental Management”)[Arc trans2]

(3) Person Responsible for Operational Management of Personal Information (hereinafter “Person Responsible for Operational Management”)[Arc trans3]

2. On behalf of the Foundation, the Chancellor and Chair acts as the Person Responsible for Overall Management, and shall have responsibility and authority over all protection of Personal Information at the Foundation, including at the Schools.

3. The chief administrative officer of each School acts as the Person Responsible for Departmental Management, and is responsible for handling the responsibilities stipulated by the preceding provision in the corresponding department.

4. The manager of the General Affairs Department of the Headquarters of the Foundation acts as the Person Responsible for Operational Management, and is responsible for managing the Personal Data and Personal Information Databases, etc. that they oversee, and for properly handling and processing requests from the applicable person(s) regarding the Retained Personal Data.

Chapter 2 The Personal Information Protection Committee

Article 6: Establishment of the Committee

The Personal Information Protection Committee (hereinafter the “Committee”) shall be established to deliberate over important matters related to the protection of Personal Information at the Foundation. The Committee shall be held as needed when meetings of the Executive Board are held.

Article 7: Matters for Deliberation

The Committee shall deliberate over the following matters.

(1) Matters related to measures the Foundation should take regarding the protection of personal information

(2) Matters raised by persons responsible regarding the acquisition, use, provision, disclosure, correction, suspension of use, and other actions pertaining to personal information

(3) Other important matters regarding the protection of personal information

Article 8: Hearing Opinions of the Information Systems Department

1. When deliberating on the handling of personal information in information systems at the Foundation, the Committee shall hear the opinions of the department in charge of information systems.

2. Aside form the provisions of the preceding paragraph, the Committee may also request opinions from relevant departments within the Foundation when deliberating on matters stipulated in the preceding article.

Article 9: Composition

The Committee shall be composed of the following members.

(1) Attendees of meetings of the Executive Board

(2) Those other than (1) above who are designated by the chairperson

Article 10: Chairperson and Vice-Chairpersons

1. The Committee shall have a chairperson, the role of which shall be served by the chairperson of the Executive Board.

2. The Committee shall have a number of vice-chairpersons who are nominated by the chairperson.

3. Vice-chairpersons shall assist the chairperson, and shall assume the duties of chairperson when that person is unable due to unforeseen circumstances.

Article 11: Meetings

1. The chairperson shall convene the Committee.

2. If at least two-thirds of committee members are not in attendance, meetings cannot be held and resolutions cannot be passed.

3. Resolution on agenda items in the Committee shall be determined by a majority vote of members in attendance. In the event of a tie, the chairperson shall cast the deciding vote.

4. Those other than the members may be allowed to attend the meetings and their opinions may be requested when deemed necessary by the chairperson.

Article 12: Administrative Office

The General Affairs Department at the Foundation’s headquarters shall conduct administrative work for the Committee.

Chapter 3 Acquisition and Use of Personal Information

Article 13: Purpose of Use

1. Personal information shall only be handled for the purposes of carrying out the work operations of the Foundation and the educational and research activities of the Schools, and the purpose of use (hereinafter the “Purpose of Use”) must be identified as specifically as possible when acquiring personal information.

2. When changing the Purpose of Use, the purpose may not be changed beyond what can reasonably be considered related to what the Purpose of Use was before the change.

Article 14: Declaring, Clarifying, and Notifying About the Purpose of Use

1. The Purpose of Use for Personal Information must either be announced or expressed to the Applicable Person(s) before acquisition, or either informed to the Applicable Person(s) or announced immediately after acquisition.

2. When changing the Purpose of Use, the Purpose of Use after the change must either be announced or informed to the Applicable Person(s) in advance.

3. The provisions of paragraph 1 and 2 above shall not apply in any of the following cases.

(1) When the life, safety, assets, or other rights or interests of the Applicable Person(s) or a third party could be threatened due to the Purpose of Use being announced or informed to the Applicable Person(s)

(2) When the rights or legitimate interests of the Foundation could be endangered by the Purpose of Use being announced or informed to the Applicable Person(s)

(3) When needing to cooperate with statutory duties performed by a national government agency or local government, and announcing the Purpose of Use or informing it to the Applicable Person(s) could hinder the performance of those duties

(4) When the state in which the personal information is acquired makes the Purpose of Use obvious

Article 15: Acquisition of Personal Information

Personal information must only be acquired to the extent necessary for achieving the Purpose of Use, and through methods that are legal and fair.

Article 16: Limitations on Acquisition

1. Personal information may not be acquired for the purposes of matters related to thoughts, beliefs, or religion, or to investigate matters that give rise to social discrimination.

2. Prior consent must be obtained from the Applicable Person(s) when acquiring Sensitive Personal Information. However, this shall not necessarily apply in any of the following cases.

(1) When acquisition of the information is based on laws or regulations

(2) When necessary to protect someone’s life, safety, or assets, and it is difficult to

obtain the consent of the Applicable Person(s)

(3) When necessary for improving public health or promoting healthy upbringing of children and/or students, and it is difficult to obtain the consent of the Applicable Person(s)

(4) When needing to cooperate with statutory duties performed by a national government agency or local government, or someone contracted to perform such duties, and obtaining the consent of the Applicable Person(s) could hinder the performance of those duties

(5) When the corresponding Sensitive Personal Information must be handled for academic research purposes (including cases in which handling the corresponding Sensitive Personal Information is partially for academic research purposes, but excluding cases in which the rights or interests of individuals could be improperly violated)

(6) When acquiring the corresponding Sensitive Personal Information from academic research institutions or other such organizations, and the corresponding Sensitive Personal Information must be acquired for academic research purposes (including cases in which acquiring the corresponding Sensitive Personal Information is partially for academic research purposes, but excluding cases in which the rights or interests of individuals could be improperly violated)

(7) When the corresponding Sensitive Personal Information is published at the direction of the Applicable Person(s) or a national government agency, local government, or others designated by the personal information-related laws or regulations

(8) When acquiring Sensitive Personal Information which can clearly be discerned from the appearance of the applicable person(s) by viewing or photographing them

(9) When there is an inevitable, justifiable reason in terms of operations at the Foundation or education and research at the Schools other than the provisions of the preceding items

Article 17: Usage of Personal Information

When using personal information, the usage may not exceed the necessary scope for achieving the Purpose of Use specified in the provisions of Article 13. However, this shall not necessarily apply in any one of following cases.

(1) When the applicable person(s) has given consent

(2) When based on laws or regulations

(3) When necessary to protect someone’s life, safety, or assets, and it is difficult to obtain the consent of the Applicable Person(s)

(4) When necessary for improving public health or promoting healthy upbringing of children and/or students, and it is difficult to obtain the consent of the Applicable Person(s)

(5) When needing to cooperate with statutory duties performed by a national government agency or local government, or someone contracted to perform such duties, and obtaining the consent of the Applicable Person(s) could hinder the performance of those duties

(6) When the Personal Information must be handled for the purpose of providing it to be used in academic research (including cases in which handling the corresponding Personal Information is partially for academic research purposes, but excluding cases in which the rights or interests of individuals could be improperly violated.)

(7) When providing personal data for academic research purposes to universities or other institutions, groups, or person(s) belonging to any of these (hereinafter “Academic Research Institutions, etc.”) and that Academic Research Institution must handle the corresponding personal data for academic research purposes (including cases in which handling the corresponding personal information is partially for academic research purposes, but excluding cases in which the rights or interests of individuals could be improperly violated.)

Article 18: Prohibition of Improper Use

The Foundation may not use Personal Information in ways that recommend or provoke illegal or unjust behavior.

Chapter 4 Management of Personal Data

Article 19: Management of Personal Data

The Person Responsible for Operational Management must manage the following to ensure the security and reliability of Personal Data.

(1) Taking the necessary measures including information security measures to prevent leakage, loss, damage, and tampering of Personal Data as well as unauthorized access thereto.

(2) Striving to keep personal data accurate and up-to-date within the necessary scope according to its Purpose of Use.

(3) Personal Data must be swiftly and reliably deleted or disposed of once no longer needed.

Article 20: Role of the Information Systems Department

The department in charge of information systems at the Foundation shall take sufficient technological safety measures to address risks such as unauthorized access to Personal Data and Personal Information Databases, etc.

Article 21:　Publishing Information about Retained Personal Data

The Foundation must make the following available for the Applicable Person(s) to know (including answering without delay when asked by that Applicable Person(s)) regarding the Retained Personal Data in its possession.

(1)　The department managing the Retained Personal Data, the title and address of the Person Responsible for Operational Management, and the name of the Foundation's representative

(2)　The Purpose of Use of all Retained Personal Data (excluding either of the cases described in Article 14, Paragraph 3, Items 1 through 3)

(3)　Procedures such as for disclosure as stipulated in Article 32

(4)　The department in charge of handling inquiries or complaints regarding the handling of Retained Personal Data stipulated in Articles 36 and 37

Article 22: Management of Contractors, etc.

1. When contracting all or part of the handling of Personal Data to a third-party contractor, the Person Responsible for Operational Management must supervise the contractor as necessary and appropriate to ensure the secure management of the Personal Data being contracted.

2. In situations described in the preceding paragraph, the following items must be listed in the corresponding contracts or other documents. However, items which are recognized as unnecessary in light of the details or nature of the work being contracted need not be listed.

(1)　The Contractor must not allow its employees to leak or steal the Personal Information learned through their handling of the corresponding Personal Data.

(2)　Prior written consent must be received from the Foundation when subcontracting the handling of the corresponding Personal Data. The same applies when re-subcontracting to an additional subcontractor.

(3)　Duration of contracting agreement

(4)　Properly and reliably either return the Personal Data or have the contractor delete or dispose of it once the Purpose of Use has been achieved

(5)　Prevent or restrict the contractor from processing (excluding that which is within the scope of the contracting agreement), tampering with, or performing other such actions with the Personal Data

(6)　Prevent duplication or replication of Personal Data by contractors (except when recognized in the contracting agreement, including for the purpose of backups necessary for secure management)

(7) Accountability to the Foundation whenever incidents such as leakages of Personal Data have occurred at contractors

(8) Responsibility of contractors whenever incidents such as leakages of Personal Data have occurred at contractors

Article 23: Supervision of External Personnel

The provisions of paragraph 1 of the preceding article shall apply mutatis mutandis when accepting personnel from the outside to perform operations including handling personal information.

Article 24: Measures when Leakages Are Discovered

1. Officers, faculty and staff members, and others at the Foundation must immediately report to the Person Responsible for Operational Management when realizing that incidents such as leakages of Personal Information or its usage for inappropriate purposes have occurred.

2. When the Person Responsible for Operational Management has received a report as described in the preceding paragraph, that person must immediately report to the Person Responsible for Overall Management via the Person Responsible for Departmental Management, confer about how to respond, and take the necessary and appropriate measures.

3. In the case described in the preceding paragraph, the Person Responsible for Overall Management shall convene the Committee as needed.

Article 25: Reporting Leakages, etc.

1. When leakage, loss, damage, or other circumstances relevant to ensuring the security of Personal Data which meet those stipulated in the Personal Information Protection Committee Rules (hereinafter the “Protection Committee Rules”) with a high likelihood of violating the rights or interests of individuals have occurred to Personal Data being handled, the Foundation must report the occurrence of those circumstances to the Government of Japan’s Personal Information Protection Commission as provided in the Protection Committee Rules.

2. When a situation occurs as described in the preceding paragraph, the Foundation must swiftly inform the relevant Applicable Person(s) of its occurrence as provided in the Protection Committee Rules. However, this shall not necessarily apply when taking alternative measures necessary to protect the rights and interests of the Applicable Person(s) in cases where it is difficult to inform that Applicable Person(s).

Chapter 5 Provision, etc., of Personal Data

Article 27: Provision of Personal Data to Third Parties

1. Personal data may not be provided to third parties without obtaining the prior consent of the Applicable Person(s). However, this shall not necessarily apply in any one of following cases.

(1) When based on laws or regulations

(2) When necessary to protect someone's life, safety, or assets, and it is difficult to obtain the consent of the Applicable Person(s)

(3) When necessary for improving public health or promoting healthy upbringing of children and/or students, and it is difficult to obtain the consent of the Applicable Person(s)

(4) When needing to cooperate with statutory duties performed by a national government agency or local government, or someone contracted to perform such duties, and obtaining the consent of the Applicable Person(s) could interfere with the performance of those duties

2. Notwithstanding the provisions of the preceding paragraph, when it has been decided at the request of applicable person(s) to suspend provision to a third party of Personal Data that could identify that Applicable Person(s), the data may be provided to a third party after informing the Applicable Person(s) in advance of the following, or after obtaining approval from the Person Responsible for Overall Management in situations when the Applicable Person(s) can readily know about the circumstances. However, this shall not necessarily apply when the Personal Data provided to a third party is Sensitive Personal Information or was acquired in violation of the provisions of Article 15 or 16.

(1) The name of the person responsible for managing that Personal Data provided to a third party, or the title, address, plus the name of a representative if a corporate entity is responsible

(2) That provision to a third party is the intended Purpose of Use

(3) Items of Personal Data that are provided to a third party

(4) Method of acquiring Personal Data that is provided to a third party

(5) Method of provision to a third party

(6) That provision to a third party of Personal Data that could identify Applicable Person(s) is suspended when requested by that Applicable Person(s)

(7) Method of accepting requests from the Applicable Person(s)

(8) Other matters necessary for protecting the rights and interests of individuals

3. If there has been a change to information in Item 1 of the preceding paragraph or if provision of the Personal Data specified in the preceding paragraph has been discontinued, such change or discontinuation shall, without delay, be informed to Applicable Person(s) or made available where the Applicable Person(s) can readily know about it. Also, when

attempting to change the information stipulated in items 3 through 5, 7 or 8, the intended change must either be informed to Applicable Person(s) in advance or made available where the Applicable Person(s) can readily know about it.

4. In the following cases, someone who receives provision of Personal Data shall not be considered a third party in applying the provisions of the preceding paragraphs.

(1) When Personal Data is used within the necessary scope for achieving the Purpose of Use by a department or division within the Foundation other than the department or division that acquired the Personal Data

(2) When Personal Data is provided along with the Foundation contracting out all or part of the handling of that Personal Data to an outside business operator or other contractor within the necessary scope for achieving the Purpose of Use

(3) When Personal Data used jointly with a specific person is provided to that specific person, and the followings have been informed to Applicable Person(s) in advance, or made available where the Applicable Person(s) can readily know about it ;

－the provision of Personal Data is to a specific person with whom the Personal Data is to be used jointly

－items of Personal Data being jointly used

－scope of persons jointly using the data

－Purpose of Use of those users

－the name of the person responsible for managing that Personal Data or the title, address, plus the name of a representative if a corporate entity is responsible

5. When there has been a change to the Purpose of Use of the users stipulated in Item 3 of the preceding paragraph or a change to the name, title, or address of the person responsible for managing that personal data or the name of the representative if a corporate entity is responsible, such change(s) shall, without delay, be informed to Applicable Person(s) or made available where the Applicable Person(s) can readily know about it. Also, when attempting to change the same, such intended change shall, in advance, be informed to Applicable Person(s) or made available where the Applicable Person(s) can readily know about it

Article 28: Restrictions on Provision to an Overseas Third Party

1. When providing Personal Data to an overseas third party, prior consent to that provision must be received from the Applicable Person(s) except in cases described in the items under Paragraph 1 of the preceding article. In such cases, the provisions of the preceding article shall not apply.

2. When attempting to gain consent from the Applicable Person(s) according to the

provisions of the preceding paragraph, the Foundation must provide that Applicable Person(s) with information in advance including the systems for protecting personal information in those countries and the personal information protection measures being taken by that third party.

3. When having provided personal data to an overseas third party, the Foundation must take the necessary measures to ensure the continuous implementation of commensurate measures by that third party, and must also provide information about those necessary measures to the Applicable Person(s) on request by the Applicable Person(s).

Article 29: Creating Records of Provision to Third Parties

1. When Personal Data has been provided to a third party, records of information including the date that Personal Data was provided and the name or title of the third party, etc. must be created. However, this shall not necessarily apply when the provision of that Personal Data corresponds to any of the cases described in the items under Article 27, Paragraphs 1 or 4.

2. The records described in the preceding paragraph must be saved for a period of three years from the date they were created.

Article 30: Checking When Receiving what Third Parties Provide, etc.

1. The items listed below must be checked when receiving Personal Data provided by a third party. However, this shall not necessarily apply when the data that is provided corresponds to any of the cases described in the items under Article 27, Paragraphs 1 or 4.

(1) The name of that third party or their title, address, plus name of a representative if it is a corporate entity

(2) The sequence of events in which that third party acquires the Personal Data in question

2. When checking as stipulated in the preceding paragraph, records must be created of information including the date provision of the personal data was received and matters related to the checks that were performed.

3. The records described in the preceding paragraph must be saved for a period of three years from the date they were created.

Chapter 6 Personal Data-Related Requests, etc.

Article 31: Requests for Purpose of Use Notifications

When the Foundation receives a request from Applicable Person(s) for notification of the Purpose of Use for Retained Personal Data that identifies that Applicable Person(s), it must

inform that Applicable Person(s) of the Purpose of Use without delay. However, this shall not necessarily apply in any one of following cases.

(1) The Purpose of Use for Retained Personal Data that can identify Applicable Person(s) is known

(2) When any of Items 1 through 4 under Article 14 Paragraph 3 apply

2. When the Foundation has decided not to inform the Purpose of Use of this Retained Personal Data based on the proviso of the preceding paragraph, the Applicable Person(s) must be informed of that fact along with the reason without delay.

Article 32: Disclosure Requests

1. The Applicable Person(s) shall be able to request that the Foundation provide disclosure of Retained Personal Data that identifies that Applicable Person(s) through methods including provision of electronic records.

2. When the Foundation receives a request based on the preceding paragraph, it must without delay disclose the corresponding Retained Personal Data to the Applicable Person(s) who made the request. In principle, the method of disclosure shall be the method requested by that Applicable Person(s), but when there are reasonable grounds, disclosure may be sent in document form instead.

3. Not disclosing all or part of the corresponding Retained Personal Data shall be possible in any one of following cases when disclosing Retained Personal Data to the Applicable Person(s) based on the preceding paragraph.

(1) When the life, safety, assets, or other rights or interests of the Applicable Person(s) or a third party could be threatened

(2) When it could significantly interfere with the proper functioning of operations at the Foundation

(3) When it would violate laws or regulations, etc.

4. When the Foundation has chosen not to disclose all or part of the corresponding Retained Personal Data or when that data does not exist, the Foundation must inform the Applicable Person(s) of that fact and also the reason without delay.

Article 33: Requests for Corrections, etc.

Article 33: When the information in Retained Personal Data that identifies Applicable Person(s) is incorrect, that Applicable Person(s) may request that the Foundation correct, add, or delete (hereinafter “Corrections, etc.”) the information in that Retained Personal Data.

2. When the Foundation receives a request based on the preceding paragraph, it must conduct the necessary investigation without delay, and based on the results, must make

Corrections, etc. to the content of the corresponding Retained Personal Data. However, this shall not necessarily apply when the results of investigations recognize that Corrections, etc. are not warranted.

3. When the Foundation has made Corrections, etc. to the corresponding Retained Personal Data based on the text in the preceding paragraph it must without delay inform the Applicable Person(s) of that fact, or inform Applicable Person(s) of that fact and the reason when it has decided not to make Corrections, etc. based on the proviso of the preceding paragraph.

Article 34: Requests to Suspend Usage, etc.

1. When the corresponding Retained Personal Data that identifies Applicable Person(s) was acquired in violation of the provisions of Articles 14, 15, or 16, or handled in violation of the provisions in Article~~s~~ 17 or 18, that Applicable Person(s) may request that the Foundation suspend usage of the corresponding Retained Personal Data or delete it (hereinafter “Suspend(ed) Usage, etc.”).

2. When receiving a request based on the preceding paragraph and when that request is determined to have reasonable grounds, the Foundation must without delay Suspend(ed) Usage etc. of the corresponding Retained Personal Data to the extent necessary to remediate the violation.

3. The Applicable Person(s) may request that the Foundation suspend provision of the corresponding Retained Personal Data to a third party when that Retained Personal Data which could identify that Applicable Person(s) is being provided in violation of the provisions of Article 27, Paragraph 1 or Article 28.

4. When receiving a request as stipulated in the preceding paragraph and when that request is determined to have reasonable grounds, the Foundation must without delay suspend provision of the corresponding Retained Personal Data to the third party.

5. The Applicable Person(s) shall be able to request that the Foundation Suspend(ed) Usage, etc. of the Retained Personal Data, or suspend its provision to a third party, when a situation stipulated in Article 25 Paragraph 1 occurs related to Retained Personal Data that identifies that Applicable Person(s) or in other such circumstances when handling the corresponding Retained Personal Data that identifies that Applicable Person(s) could harm the rights or interests of that Applicable Person(s).

6. When receiving a request as stipulated in the preceding paragraph and when that request is determined to have reasonable grounds, the Foundation must without delay Suspend(ed) Usage, etc. of the Retained Personal Data or suspend its provision to a third party to the extent necessary to prevent harming the rights or interests of the Applicable Person(s).

7. When it is difficult for the Foundation to Suspend Usage, etc. of the Retained Personal

Data or suspend its provision to a third party as stipulated in Paragraphs 2, 4, and 6 above due to high cost or other such reasons, the sufficient measures necessary to protect the rights and interests of the Applicable Person(s) may be taken in lieu of the corresponding Suspend(ed) Usage, etc. or suspending provision to a third party.

8. When the Foundation has Suspend(ed) Usage, etc. of all or part of the corresponding Retained Personal Data or suspended its provision to a third party based on the provisions of Paragraphs 2, 4, or 6, the Foundation must without delay inform the Applicable Person(s) of having done so. Additionally, when the Foundation has taken measures in lieu of Suspend(ed) Usage, etc. or suspending provision to a third party based on the provisions of Paragraph 7, the Foundation must without delay inform the Applicable Person(s) of having done so, and the reason.

Article 35: Procedures for Disclosure, etc.

1. When sending a request based on the provisions of Articles 31 through 34 (hereinafter “Request for Disclosure, etc.”), the Applicable Person(s) must clarify their identity, enter the required information on the designated form and submit it addressed to the person responsible for handling the requests.

2. The person responsible for handling the requests may require that Applicable Person(s) enter sufficient information in the Request for Disclosure, etc. to identify either the applicable Retained Personal Data or the third-party disclosure record.

Chapter 7　Appeals and Handling of Complaints

Article 36:　Appeals

1. When the Applicable Person(s) who made a Request for Disclosure, etc. disagrees with the measures taken by the Foundation based on that request, the Applicable Person(s) may appeal to the Committee.

2. When appealing as described in the preceding paragraph, the Applicable Person(s) shall submit the clarification of their identity and form containing the entered information required for the appeal to the department that manages the applicable Retained Personal Data, which shall be submitted to the Committee via the corresponding Person Responsible for Operational Management and Person Responsible for Departmental Management.

3. When there has been an appeal as stipulated in Paragraph 1, the Committee shall deliberate and inform the appellant(s) of the result in writing.

4. When deliberating on an appeal, the Committee may require the appellant(s), the Person Responsible for Operational Management, the Person Responsible for Departmental Management, faculty and staff members in related departments, and/or other related parties

to attend a Committee meeting or submit a written statement when deemed necessary.

Article 37: Handling Complaints, etc.

1. The department in charge of the applicable Retained Personal Data shall serve as the contact point for inquiries and complaints about Retained Personal Data and handle those inquiries and complaints.

2. Despite the provisions of the preceding paragraph, the General Affairs Department at the Foundation's headquarters shall handle the inquiry or complaint when the department in charge of the corresponding Retained Personal Data cannot be identified or when the inquiry or complaint pertains to general handling of personal information at the Foundation.

Chapter 8 Supplementary Provisions

Article 38: Disciplinary Action

When violations of these Rules are discovered, the Foundation may subject those involved in those violations to disciplinary action based on the relevant rules.

Article 39: Administrative Office

The General Affairs Department at the Foundation's headquarters shall perform administrative work pertaining to these Rules.

Article 40: Revision and Abolition Procedures

These Rules shall be revised or abolished by the Chancellor upon deliberations by the Executive Board.

Supplementary Provisions

These revised rules shall come into effect as of June 28, 2024.