* The Japanese version is the authoritative version, and this English translation is intended for reference purposes only. Should any discrepancies or doubts arise between the two versions, the Japanese version will prevail.

The University of Tokyo Rules for the Handling of Personal Information, etc.

Established on March 17, 2005
Board Resolution
The University of Tokyo Rules No. 333

Chapter 1. General Provisions

(Purpose)

Article 1.

The purpose of these Rules is to protect the rights and interests of individuals while ensuring the proper and smooth operation of affairs and businesses of The University of Tokyo (hereinafter referred to as the "University"), in view of a significant increase in the use of personal information and other information relating to an individual at the University.

(Definitions)

Article 2.

The definitions of the terms used in these Rules shall be governed by the Act on the Protection of Personal Information (Act No. 57 of 2003; hereinafter referred to as the " Personal Information Protection Act") and the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (Act No. 27 of 2013; hereinafter referred to as the "Numbers Act") and other relevant laws and regulations.

Chapter 2. Management System for Personal Information etc.

(Senior Protection Manager)

Article 3.

1. One senior protection manager shall be appointed at the University, and an executive staff designated by the president shall serve as the senior protection manager.
2. The senior protection manager shall supervise affairs related to the proper handling of information defined by the Personal Information Protection Act, such as personal information pseudonymous processing information, anonymized processing information, information relating to individuals, and other information that is subject to the Act and is defined by the Personal Information Protection Act and the Act on the Individual Numbers (hereinafter referred to as “personal information, etc.”).
3. The senior protection manager shall be responsible for ensuring the proper handling of personal information, etc. at the University as follow.
   (1) Interpretation and operation of these Rules
   (2) Establishing a management system for personal information, etc. at the University

(3) Formulation, revision or abolition of these Rules and other rules and regulations concerning the handling of personal information, etc. at the University

(4) Guidance, advice and supervision with regards to Paragraph 2, Items 2, 4 and 6 of Article 4 at each Faculty/Graduate School stipulated in Paragraph 1 of the same article

(5) Response to reports and consultations from the Organization Senior Protection Managers

(6) In addition to what is listed in the preceding items, services provided for in the rules and regulations concerning the handling of personal information, etc. at the University.

4. The senior protection manger may investigate each organization when it is deemed necessary for the management of personal information, etc.

5. The senior protection manager shall organize the general protection management committee and represent it as its chairperson. In such case, the general protection management committee shall be deemed to be in charge of the duties set forth in the preceding two paragraphs.

6. The senior protection manager shall provide for the matters necessary concerning the operation of the general protection management committee.

(Organization Senior Protection Managers)

Article 4.

1. One organization senior protection manager shall be appointed at each organization or any other division (i.e. university academic organizations, university library systems, the University of Tokyo Archives, the university joint education and research institutes, research institutions and Tokyo College established at the University of Tokyo Institutes for Advanced Study (UTIAS), the interdisciplinary research institutes, the national joint-use institutes, the collaborative research organizations, the Secondary School attached to the Faculty of Education, the University of Tokyo Hospital, Research Hospital, Institute of Medical Science and divisions; the same shall apply hereinafter), and heads of the respective organizations or other divisions or substitute persons (general managers and the manager of internal audit group in the case of divisions) shall serve as organization senior protection managers.

2. Organization senior protection managers shall take charge of ensuring the proper management of the personal information, etc. at each organization or any other divisions, and shall be in charge of the following duties.

(1) Establish a system for the management of personal information, etc. in the organizations or other divisions

(2) Formulation, revision and abolition of the detailed regulations of the relevant organization or division pertaining to these rules

(3) Appointment and supervision of protection managers

(4) Understanding and supervision of the status of the management of personal information, etc. in the relevant organization or division

(5) Reporting and consultation on necessary matters concerning the proper management of personal information, etc. to the senior protection manager

(6) In addition to what is listed in the preceding items, services provided for in the rules and regulations concerning the handling of personal information, etc. at the University.

3. The organization senior protection manager may, conduct necessary investigation concerning the management of personal information, etc. in their relevant organization or division if deemed necessary.

4. When multiple organizations or divisions are involved in the handling of personal information, etc., the organization senior protection managers of each organization or division shall be responsible for the handling of personal information, etc. in collaboration with each other and shall be jointly responsible under Paragraph 2.

(Protection Managers)

Article 5.

1. One or more protection managers shall be appointed at each organization or division designated by the relevant organization senior protection manager.

2. Protection managers shall assist the organization senior protection managers and shall be in charge of the following duties with regards to the proper management of personal information, etc. relating to the relevant organizations or divisions.

(1) Appointment and supervision of protection officers and administration officers

(2) Reporting and consulting on necessary matters concerning the management of personal information, etc. to the organization senior protection manager

(3) In addition to what is listed in the preceding items, the services provided for in the rules and regulations concerning the handling of personal information, etc. at the University.

3. When handling personal information, etc. using an information system, the protection manager shall be in charge while cooperating with the manager of the information system.

4. When multiple organizations or divisions are involved in the handling of personal information, etc., the protection manager of each organization or division shall assist the organization senior protection manager of the organization or division to which they are affiliated.

(Protection Officers)

Article 6.

1. One or more protection officers shall be appointed by the relevant protection manager at each organization or division.

2. The protection officers shall assist protection managers and shall be in charge of the following duties with regards to the proper management of the Personal Information, etc. at each organization or division.

(1) General affairs concerning the management of personal information, etc. (excluding the Individual Number set forth in Article 2, Paragraph 5 of the Numbers act and specific personal information set forth in same shall apply in this paragraph)

(2) Reporting and consulting on necessary matter for the management of personal information, etc. to the protection manager

(3) In addition to what is listed in the preceding items, the services provided for in the rules and regulations concerning the handling of personal information, etc. at the University.

(Administration Officers)

Article 7.

1. Protection managers shall appoint one or more staff members (hereinafter referred to as the "administration officer") who handle specific personal information, etc.

2. Protection managers shall specify the extent to which specific personal information, etc. is to be handled by each administration officer.

(Establishment of Systems for Specific Personal Information, etc.)

Article 8.

Protection managers shall establish the following systems for specific personal information, etc.:

(1) a communication system that allows an administration officer, who has become aware of facts relating to the breach (or signs of the occurrence of a breach) of the provisions of related laws, regulations, rules and the like, to report the matter to the protection manager

(2) a communication system that allows executive, academic and administrative staff members (including dispatched workers; hereinafter referred to as "academic and administrative staff"), who have become aware of the occurrence or signs of occurrences of incidents such as leaks, loss or damage of specific personal information, etc. (hereinafter referred to as "leakage, etc."), to report to the protection manager

(3) clarification of the allocation of duties and responsibilities of the respective organizations where specific personal information, etc. is handled by multiple departments, and

(4) a response system when becoming aware of the occurrence or sign of incidents such as leakage, etc. of specific personal information, etc.

(Organizations, etc. Pertaining to Disclosure Requests)

Article 9.

The University of Tokyo Information Disclosure Committee shall be entrusted with disclosures etc. of personal information at the University in accordance with the rules separately provided.

(General Auditor)

Article 10.

1. One general auditor shall be appointed at the University, and the executive vice president or vice president responsible for internal auditing shall serve as the general auditor.

2. The general auditor shall take charge of audits of the management status of the personal information, etc.

3. The general auditor may conduct necessary audits of the management of personal information, etc. of each organization or division when deemed necessary.

Chapter 3. Formulations of Regulations Regarding the Handling of Information in Academic Research

Article 11.
1. The general protection management committee shall, when handling personal information, etc. (excluding specific personal information, etc.; hereinafter the same shall apply in this paragraph) for academic research purposes, establish rules concerning the handling of personal information, etc. for said academic research purposes in cooperation with the organizations and other divisions that intend to handle personal information, etc. for said academic research purposes, and shall take necessary measures to ensure the implementation of the matters specified in said rules.
2. The general protection management committee shall endeavor to publicize the contents of the rules prescribed in the preceding paragraph and the measures to be taken.

Chapter 4. Education and Training

Article 12.
The senior protection manager shall provide all academic and administrative staff who handle personal information, etc. with awareness-related training and other necessary education and training, aiming to deepen their understanding of the handling of personal information, etc. and increase awareness about the protection of personal information, etc.

Article 13.
The senior protection manager shall provide all academic and administrative staff engaged in affairs relating to the administration of information systems handling of personal information, etc. with the education and training necessary for the administration, operation and formulation of security countermeasures of information systems for the proper management of personal information, etc.

Article 14.
The senior protection manager shall provide organization senior protection managers, protection managers, protection officers and administration officers with the education and training for the proper management of personal information, etc. at the sites of organizations or other divisions.

Article 15.
Organization senior protection managers and protection managers shall take necessary measures for the proper management of personal information, etc. for the benefit of academic and administrative staff of organizations or

other divisions including the granting of opportunities to participate in the education and training provided by the senior protection manager.

Chapter 5. Responsibilities of Academic and Administrative Staff

Article 16.

1. Academic and administrative staff must handle personal information, etc. in conformity with the purport of the Incorporated Administrative Agencies Personal Information Protection Act and the Numbers Act, and in compliance with the provisions of related laws, regulations, rules and the like, as well as the instructions of the senior protection manager, organization senior protection managers, protection managers, protection officers and administration officers.

Article 17.

Academic and administrative staff shall not, without due cause, inform other of the contents of personal information, etc. they have come to know in the course of performing their duties, or use it for unjust purposes.

Chapter 6. Handling of Personal Information, etc.

(Specification of the Purpose of Use)

Article 18.

1. When handle personal information, academic and administrative staff shall specify the purpose of use (hereinafter referred to as the "Purpose of Use") only in the cases where it is necessary to perform affairs handling the said personal information.
2. Academic and administrative staff shall not change the purpose of use beyond the scope that is reasonably considered to be related to the purpose of use before the change.

(Restrictions from the Purpose of Use)

Article 19.

No academic or administrative staff shall handle personal information beyond the scope necessary for achieving the purpose of use specified pursuant to the provisions of the preceding article, except in the following cases.

(1) In accordance with laws and regulations
(2) Cases in which the provision of personal information is necessary for the protection of life, body or property of an individual, and in which it is difficult to obtain the consent of the individual
(3) Cases in which the provision of personal information is necessary to improve public health or promote the sound growth of children, and in which it is difficult to obtain the consent of the individual
(4) Cases in which the handling of personal information is necessary to cooperate with a state organization, local government or an individual or business operator entrusted by either of the

former two in executing the affairs prescribed by laws and regulations, and in which obtaining the consent of the individual would likely impede the execution of the affairs concerned

(5) When it is necessary to handle the personal information for academic research purposes (hereinafter referred to as "academic research purposes") (including cases where part of the purpose of handling the said personal information is for academic research purposes, and excluding cases where it is likely to infringe the rights and interests of the individuals)

(6) When personal information is provided to universities, other institutions or organizations aimed at academic research, or persons affiliated with them (hereinafter referred to as "academic research institutions, etc."), and where said academic research institutions, etc. need to handle said personal information for academic research purposes (including cases where part of the purpose of handling said personal information is an academic research purpose, but excluding cases where the rights and interests of individuals are likely to be unreasonably infringed).

2. Academic and administrative staff shall obtain prior consent from the individual in question when handling personal information beyond the scope of the purpose of use specified pursuant to the provisions of the preceding article.

(Notification of the Purpose of Use at the Time of Acquisition, etc.)

Article 20.

1. When academic and administrative staff acquire personal information, they shall promptly notify the individual or publicly announce the purpose of use, except in cases where the purpose of use has been publicly announced in advance.

2. Notwithstanding the provisions of the preceding paragraph, in cases where academic and administrative staff acquire personal information of an individual that is stated in a contract or other documents (including electronic records) as a result of concluding a contract with said individual or otherwise acquires their personal information that is recorded from a document directly from the individual, the academic and administrative staff shall clearly indicate the purpose of use in advance to the individual.

3. If academic and administrative staff changes the purpose of use, they shall notify the individual of the changes to the purpose of use or announce it publicly.

4. The provisions of the preceding three paragraphs shall not apply in the following cases.

(1) If notifying the individual of the purpose of use or publicly announcing it is likely to harm the life, body, property or other rights or interests of the individual or a third party

(2) If notifying the individual of the purpose of use or publicly announcing it is likely to harm the rights or legitimate interests of the University

(3) Where it is necessary to cooperate with a state organization or a local government in executing the affairs prescribed by laws and regulations and in which notifying the person of the purpose of use or publicly announcing it are likely to impede the execution of the affairs

(4) Where it is considered that the purpose of use is clear in consideration of the circumstances of the acquisition.

(Prohibition of Improper Use)

Article 21.

Academic and administrative staff shall not use the personal information in a manner that encourages or is likely to induce illegal or unjust acts.

(Appropriate Acquisition of Information)

Article 22.

1. Academic and administrative staff shall not obtain personal information by deception or other wrongful means.

2. No academic or administrative staff shall acquire personal information requiring consideration without obtaining the prior consent of the individual, except in the following cases.

(1) In accordance with laws and regulations

(2) Where the provision of personal information is necessary for the protection of the life, body or property of an individual and where it is difficult to obtain the consent of the person

(3) Where the provision of personal information is specially necessary for improving public health or promoting the sound growth of children and where it is difficult to obtain the consent of the person

(4) Where the handling of personal information is necessary for cooperating with a state organization, a local government or an individual or an individual or business operator entrusted by either of the former two in executing the affairs prescribed by laws and regulations, and in which obtaining the consent of the individual would likely impede the execution of the affairs concerned

(5) When it is necessary to handle said personal information requiring consideration for academic research purposes (including cases where part of the purpose of handling the said personal information requiring consideration is for academic research purposes, and excluding cases where it is likely to infringe the rights and interests of the individuals)

(6) Where the personal information requiring consideration is to be obtained from an academic research institution etc., and where the said personal information requiring consideration is necessary for academic research purposes (including cases where part of the purpose of handling the said personal information requiring consideration is for academic research purposes, and excluding cases where it is likely to infringe the rights and interests of the individuals) (limited to cases where the said academic research institution, etc. conducts academic research jointly with the University.)

(7) Where the personal information requiring consideration is disclosed to the extent permitted under the law by the individual, national organization, local government, academic research institution, etc., press organization, person who engages commercially in writings, religious organization, political organization, foreign government, foreign governmental organization, foreign local government or an international organization, or a person who engages commercially in academic

research organization, etc., a press organization, a person who engages commercially in writings, religious organization or political organization in a foreign country

(8) Where the person obtains the personal information that is obviously necessary for consideration from viewing the individual or by taking a photograph of the individual

(9) In the cases listed in each item of Article 29, Paragraph 2 (including cases where it is applied by replacing the terms pursuant to the provision of Article 35, Paragraph 6 and the cases where it is applied by replacing the terms pursuant to Article 36, paragraph 2) when the personal information requiring consideration is the personal data provided.

(Ensuring Accuracy)

Article 23.

1. Academic and administrative staff shall endeavor to keep personal information accurate and up-to-date within the scope necessary for achieving the purpose of use, and endeavor to delete said personal information without delay when it is no longer required.
2. In the event of any errors are found in the contents of the personal information, academic and administrative staff shall make corrections etc. in accordance with the instructions of the protection officers.
3. Academic and administrative staff shall delete personal data or dispose of the media on which the personal data is stored on in a manner that makes it impossible for the personal data to be recovered or read, in accordance with the instructions of the protection manager, once the personal data or the media on which it is stored is no longer required.

(Security Control Measures)

Article 24.

1. The organization senior protection manager shall take necessary and appropriate measures to prevent the leakage, etc. of personal data being handled and for the safe management of personal data.
2. The organization senior protection manager shall establish necessary and appropriate measures for the safe management of the personal data and shall ensure that academic and administrative staff observe them.

(Contracting Out the Business etc.)

Article 25.

1. When an organization senior manager contracts out the handling of personal data, in whole or in part, they shall conduct necessary and appropriate supervision of the contracted party in order to ensure the safe management of the entrusted personal data.
2. When contracting out the handling of personal data, the protection managers shall take necessary measures, such as confirming at the time of selection, the management capability of personal data, specify the following items in the contract, and confirm in writing the necessary matters such as the status of the management of managers and employees, management of the implementation system and personal information at the contracted party.

(1) Measures equivalent to the safety management measures taken by the University shall be taken

(2) Obligations to maintain the confidentiality of personal data and prohibit the use of the personal data for other purposes

(3) Matters concerning the conditions pertaining to sub-contracting (including cases where the sub-contractor is a subsidiary of the contractor (meaning a subsidiary as prescribed in Article 2, Paragraph 1, Item 3 of the Companies Act (Act No. 86 of 2005), the same shall apply hereinafter)), such as restrictions or preapproval, etc.

(4) Matters concerning restrictions on reproduction, copying etc. of the personal data

(5) Matters concerning measures to be taken in the event of leakage, etc. of personal data (including, but not limited to, reports on the occurrence of the leakage, etc. to the protection manger by the contractor.)

(6) Matters concerning the deletion of personal data and return of the media at the time of termination of the contract

(7) Cancellation of the contract, liability for damages, and other matters necessary in the event of a violation

(8) In addition to what is listed in the preceding items, matters necessary due to the nature of handling of personal data being contracted out.

3. When outsourcing work relating to the handling of personal data, protections managers shall confirm the management and implementation system of the contracted party and the status of the management of the personal information at least once a year, in principle, through on-the-spot inspections, in accordance to the confidentiality and amount of personal information that is being outsourced.

4. In cases where the handling of the personal data is being sub-contracted out by the contractor (including cases where it is sub-sub-contracted out), the protection managers shall have the contractor implement the measure set forth in this Article, as well has have the contractors, or the protection managers themselves shall, ensure that the measures set forth in this Article is implemented in accordance with the confidentiality and quantity of the personal data being entrusted.

(Access Restriction)

Article 26.

1. Protection managers shall, according to the nature of personal data including the confidentiality thereof (including the ease of identifying the person by a degree of anonymization, the existence of personal information requiring consideration, and the nature and extent of the damage that should occur in the event of a leakage etc., the same shall apply hereinafter), limit the scope of academic and administrative staff authorized to access such personal data and the details of such authority to the minimum extent necessary for such academic and administrative staff to perform their duties.

2. Academic and administrative staff who have no access authority may not access the personal data.

3. Academic and administrative staff may not access the personal data for any purpose other than the business purposes even if he/she has access authority.

(Restriction on Reproduction, etc.)

Article 27.

With respect to the following acts, protection managers shall, according to the nature of the personal data, including the confidentiality thereof, limit the cases in which such acts are permitted to be conducted even in cases where academic and administrative staff handle such personal data for business purposes. Academic and administrative staff shall perform the following acts in compliance with the instructions of protection managers:

(1) reproduction of personal data

(2) transmission of personal data

(3) sending or taking the media containing personal data outside, and

(4) any other act that is likely to interfere with the proper management of personal data.

(Media Management, etc.)

Article 28.

Academic and administrative staff shall store media containing personal data in the designated place as instructed by a protection manager, and when deemed necessary, store the same under lock and key in a fireproof safe.

(Restriction of Provision to Third Parties)

Article 29.

1. Academic and administrative staff shall not provide personal data to third parties without obtaining the prior consent of the individual, except in the following cases.

(1) In accordance with laws and regulations

(2) When the provision of personal data is necessary for the protection of the life, body or property of an individual and when it is difficult to obtain the consent of the individual

(3) When the provision of personal data is specially necessary for improving public health or promoting sound growth of children and when it is difficult to obtain the consent of the individual

(4) When the provision of the personal data is necessary for cooperating with a state organization, local governments or an individual or an individual or business operator entrusted by either of the former two in executing the affairs prescribed by laws and regulations, and in which obtaining the consent of the individual would likely impede the execution of the affairs concerned

(5) Where the provision of said personal data is unavoidable for the purpose of publicizing or teaching the results of academic research (excluding cases where there is a risk of unreasonable infringement of the rights and interests of the individual).

(6) When it is necessary to provide said personal data for academic research purposes (including cases where part of the purpose of providing the personal data is for academic research purposes and excluding cases where there is a risk of unreasonable infringement of the rights and interests of the individual) (limited to cases where the academic research is conducted jointly by the University and said third party).

(7) Where the said third party is an academic research institution, etc. and it is necessary for said third party to handle the personal data for academic research purposes (including cases where part of the purpose of providing the personal data is for academic research purposes and excluding cases where there is a risk of unreasonable infringement of the rights and interests of the individual).

2. The person who receives such personal data shall not fall under the category of a third party with regards to the application of the provisions of the preceding paragraph in the following cases.

(1) Where the personal data is provided as a result of contracting out the handling of personal data, in whole or in part, to the extent necessary for the achievement of the purpose of use by the university

(2) Where the personal data to be jointly used with a specific individual is provided to said individual and the fact and scope of items of personal data to be jointly, the range of the persons to be use the data jointly, the purpose of use by person due to use the data jointly, and the name and address of the person who will be responsible for the management of the personal data, or in the case of a corporation, the name of a representative shall be notified in advance to the individual or made readily accessible to the individual (in the event there is a change in person who is responsible for the management of the personal data, or in the case of a corporation, there is a change in the representative, or if there is a change in the purpose of use by the specific individual provisioned in this item, or said person in charge, the individual shall be notified without delay of the intent to make the changes or made readily accessible to the individual.

(Restrictions on the Provision to Third Parties Located in Foreign Countries)

Article 30.

1. Notwithstanding the provisions of the preceding article, in cases where the University provides personal data to a third party in a foreign country or region (meaning a country or region outside the territories of Japan), academic and administrative staff shall obtain the consent of the individual in advance of the provision to a third party in a foreign is made, except in the following cases.

(1) In the event any one of the items in Paragraph 1 of the preceding article

(2) When the personal data is provided to a third party in the country stipulate by the Rules of Personal Information Protection Commission as a foreign country which has a system concerning the protection of personal data that is deemed to be at the same level as Japan in protecting the rights and interests of the individual

(3) When the personal information is provided to a third party in the country stipulated by the Rules of the Personal Information Protection Committee as a foreign country which has a system concerning the protection of personal data that is deemed to be at the same level as Japan in protecting the rights and interests of individuals.

2. Academic and administrative staff shall, when intending to obtain the consent of the individual pursuant to the provisions of the preceding paragraph, provide the individual in advance with a system for the protection of personal information in the foreign country concerned pursuant to the provisions of the Rules of the Personal

Information Protection Committee, measures to be taken by the third party for the protection of personal information and other information that will be helpful for the individual in question.
3. In the event that personal data is provided to a third party in a foreign country (limited to a person who has a system provided for in Paragraph 1, Item (3)), the academic or administrative staff shall, pursuant to the provisions of the Rules of the Personal Information Committee, take the necessary measures to ensure the continuous implementation of the appropriate measures by the third party, and at the request of the individual, provide the person with information on the necessary measures.

(Preparation, etc. of Records Pertaining to Provision to a Third Party)
Article 31.
1. When the University provides personal data to a third party, academic and administrative staff shall, pursuant to the provisions of the Rules of the Personal Information Protection Committee, prepare records concerning the date when the personal data was provided, the name of the third party, and any other matters specified by the Rules of the Personal Information Protection Committee. Provided, however, that this shall not apply where the provision of such personal data falls under any of the items of Article 29, Paragraph 1 or Paragraph 2 (in case of provisions of personal information pursuant to the provisions of Paragraph 1 of the preceding article, any of the items of Article 29, Paragraph 1).
2. Academic and administrative staff shall retain the records set forth in the preceding paragraph for a period specified by the Rules of the Personal Information Protection Committee from the date of preparation of said records.

(Confirmation upon Receiving Provision from Third Parties)
Article 32.
1. When the University receives personal data from a third party, academic and administrative staff shall confirm the following matters pursuant to the provisions of the Rules of the Personal Information Protection Committee, provided, however, that this shall not apply where the provision of such personal data falls under any of the items of Article 29, Paragraph 1 or Paragraph 2.

(1) The name and address of the third party and in the event of a corporation, the name of its representative
(2) Background as to how the third party came to acquire the personal data.

2. Academic and administrative staff shall, when they have made confirmation pursuant to the provisions of the preceding paragraph, prepare records concerning the date of receipt of the personal data, the matters pertaining to the confirmation and other matters prescribed by the Rules of the Personal Information Protection Committee, pursuant to the provision of the Rules of the Personal Information Protection Committee.
3. Academic and administrative staff shall retain the records set forth in the preceding paragraph for a period specified by the Rules of the Personal Information Protection Committee from the date of preparation of such records.

(Restrictions on Provision of Personal Information to Third Parties)

Article 33.

1. If it is assumed that a third party will acquire personal information (limited to those that constitute a personal information database, etc.) as personal data, academic and administrative staff shall not provide such personal information to such third party without obtaining prior confirmation with regards to the following matters pursuant to the Rules of the Personal Information Protection Committee, except in the cases listed in each item of Article 29, Paragraph 1.

(1) The consent of the individual concerned has been obtained to allow said third party to acquire personal information that will lead to the identification of the individual through the provision of personal information from the University

(2) Regarding the provision of personal information to a third party in a foreign country, in the case where the consent of the individual set forth in the preceding item is sought, the system for the protection of personal in the foreign country, measures for the protection of personal information to be taken by the third party, and other information that will be helpful for the person in question have been provided to the person in advance pursuant to the provisions of the Rules of the Personal Information Protection Committee.

2. When personal information is provided to a third party in a foreign country (provided, however, that this shall be limited to a person who has developed a system as prescribed in Article 30, Paragraph 1, item 3), academic and administrative staff shall, pursuant to the provisions of the Rules of the Personal Information Protection Committee, take necessary measures to ensure continuous implementation of reasonable measures by the third party.

3. In the event that academic and administrative staff have confirmed, pursuant to the provisions of Paragraph 1, the academic and administrative staff shall, pursuant to the provisions of the Rules of the Personal Information Protection Committee, prepare a record of the date when the personal information was provided, the matters pertaining to the confirmation and other necessary matters.

(Restrictions on Acquiring Related Personal Information as Personal Data)

Article 34.

1. In the event that it is assumed that the personal information to be provided by a third party will be acquired as personal data, the academic and administrative staff shall, except in the cases listed in each item of Article 29, Paragraph 1, obtain consent from the individual identified with regards to such personal data to the effect that such person will be permitted to acquire such personal information as will lead to the identification of the individual through the provision of personal information by such third party.

2. Academic and administrative staff shall, when they have obtained personal data by receiving related personal information, confirm the name and address of the third party and, in case of a corporation, the name of its representative, and record the matter listed in the following items pursuant to the provisions of the Rules of the Personal Information Protection Committee.

(1) The consent of the individual set forth in Paragraph 1, item (1) of the preceding Article has been obtained.

(2) The name and address of the third party and, in the case of a corporation, the name of its representative.

(3) The name of the person identified by said personal data and other matters sufficient for identifying said individual.

(4) Items of said personal information.

(Preparation of pseudonymous processing information, etc.)

Article 35.

1. Academic and administrative staff shall, when preparing pseudonymous processing information (limited to information that constitutes a pseudonymous processing information database, etc., the same shall apply in the following Article), process personal information in accordance with the standards provided for by the Rules of the Personal Information Protection Committee as information necessary for making it impossible to identify a specific individual unless it is collated with other information.

2. When academic and administrative staff have prepared pseudonymous processing information or have acquired pseudonymous processing information and relevant deleted information, etc. pertaining to said pseudonymous processing information (meaning descriptions, etc. deleted from personal information used in the preparation of pseudonymous processing information, personal identification codes, and information on the processing methods implemented pursuant to the provisions of the preceding paragraph), they shall take measures for safety management of the deleted information, etc. in accordance with the standards provided for in the Rules of the Personal Information Protection Committee as necessary for preventing the leakage of the deleted information, etc.

3. Academic and administrative staff shall not handle pseudonymous processing information (limited to personal information, hereinafter the same shall apply in this Article) beyond the scope necessary for achieving the purpose of use specified pursuant to the provisions of Article 18, Paragraph 1, except in the case where it is based on laws and regulations.

4. With regards to the application of the provisions of Article 20 to the pseudonymous processing information, “notify the individual, or publicly announce” in Paragraphs 1 and 3 of the same Article shall be read as “publicly announce”, and “notify the individual, or publicly announce” in Paragraph 22, items 1 through 3 of the same Article shall read as “publicly announce”.

5. When it is no longer necessary for academic or administrative staff to use the personal data or deleted information, etc. that is pseudonymous processing information, they shall endeavor to delete the said personal data or deleted information, etc. without delay.

6. Academic and administrative staff shall not provide personal data that is pseudonymous processing information to a third party except in the case of compliance with laws and regulations, notwithstanding the provisions of Article 29, Paragraph 1 and Article 30. In this case, the phrase “the preceding paragraph” in Article 29, Paragraph 2 shall be deemed to be replaced with “Article 35, Paragraph 6”. The phrase “shall be notified in advance to the individual or made readily accessible to the individual” in item (2) of the same paragraph shall be deemed to be replaced with “when they have announced publicly”. The phrase “under any of the items of Article 29, Paragraph 1 or Paragraph 2 (in case of provisions of personal information pursuant to the provisions of Paragraph 1 of the

preceding article, any of the items of Article 29, Paragraph 1)" in the proviso of Article 31, Paragraph 1 and the phrase "under any of the items of Article 29, Paragraph 1 or Paragraph 2" shall be deemed to be replaced with "under the laws and/or any of the items of Article 29, Paragraph 2".

7. Academic and administrative staff shall not, when handling pseudonymous processing information, collate the pseudonymous processing information with other information in order to identify the person pertaining to the personal information used in the preparation of the pseudonymous processing information.

8. Academic and administrative staff shall not, when handling pseudonymous processing information, use the contact information or other information contained in the pseudonymous processing information in order to make telephone calls, send correspondences by post or commercial couriers as prescribed in Article 2, Paragraph 2 of the Act of Correspondence Delivery by Private Business Operators (Act No. 99 of 2002) or general correspondence delivery operators prescribed in Paragraph 6 of the same Article or a specified correspondence delivery operator prescribed in Paragraph 9 of the same Article, or send telegraphs, facsimile or other electromagnetic means (meaning a method of using electronic data processing system or any other method using information and communications technology that is specified by the Rules of the Personal Information Protection Committee) or visit the residence.

9. The provisions of Article 18, Paragraph 2, and Articles 78 and 80 shall not apply to the pseudonymous processing information and personal data that are the pseudonymous processing information.

(Restriction of the Provision of Pseudonymous Processing Information to Third Parties)

Article 36.

1. Academic and administrative staff shall not provide pseudonymous processing information (excluding information that is personal information, hereinafter the same shall apply in this Article) to third parties, except in the case where it is based on laws and regulations.

2. The provisions of Article 29, Paragraph 2 shall apply *mutatis mutandis* to the individual who receives the information on pseudonymous processing. In this case the term "shall be notified in advance to the individual or made readily accessible to the individual" in item (2) of the same paragraph shall be deemed to be replace with "when publicly announced" and the term "shall be notified to the individual or made readily accessible to the individual" shall be deemed to be replaced with "shall be publicly announced".

3. The provisions of Articles 24 through 28 and Paragraphs 7 and 8 of the preceding Article shall apply *mutatis mutandis* to the handling of pseudonymous processing information. In this case, the term "leakage, etc." in Article 24 shall be deemed to be replaced with "leakage", and the term "for the purpose" in Paragraph 7 of the preceding Article shall be deemed to be replaced with "or obtaining deleted information, etc. for the purpose".

4. Chapter 10 shall not apply to pseudonymous processing information.

(Obligations in the Handling of Anonymized Processing Information)

Article 37.

1. Academic and administrative staff shall, when providing anonymized processing information (excluding anonymized processing information of administrative agencies, etc., hereinafter the same shall apply in this Article)

to third parties, except in cases based on laws and regulations and pursuant to the Rules of the Personal Information Protection Committee, publicize in advance the items of personal information contained in the anonymized processing information to be provided to third parties and the method of provision thereof, and clearly indicate to said third parties that the information pertaining to said provision is anonymized processing information.
2. Academic and administrative staff shall not, when handling anonymized processing information, except in cases based on laws and regulations, acquire descriptions, etc. deleted from relevant personal information, personal identification codes or information concerning the method of processing, or collate said anonymized processing information with other information in order to identify the individual concerned pertaining to the personal information used in preparing the said anonymized processing information.
3. Academic and administrative staff shall take necessary measures for the proper management of the anonymized processing information in accordance with the standards set forth in the Rules of the Personal Information Protection Committee as necessary to prevent leakage of the anonymized processing information.
4. In the event that the University outsources the handling of anonymized processing information (including two or more stages of outsourcing), academic and administrative staff shall entrust the contracted party to comply with the provisions of the preceding two paragraphs.

(Preparation and Provision of Anonymized Processing Information of Administrative Agencies, etc.)
Article 38.
1. The senior protection manager may prepare anonymized processing information of administrative agencies, etc. (limited to information that constitutes and anonymized processing information file of administrative agencies, etc.) in accordance with the provisions of Chapter 5, Section 5 of the Personal Information Protection Act.
2. The senior protection manager shall establish rules concerning the handling of anonymized processing information of administrative agencies, etc.

(Preparation and Publication of Personal Information File Register)
Article 39.
1. The organization senior protection managers shall report to the senior protection manager the contents provided separately as necessary matters for the preparation of personal information file register with regards to the handling of personal information in each organization.
2. The senior protection manager shall prepare and publish the personal information file register based on the reports pursuant to the provisions of Paragraph 1.

Chapter 7. Ensuring Security of Information Systems, etc.

(Access Control)
Article 40.
Protection managers shall take measures necessary for access control, including the setting up of functions to identify the level of authority (hereinafter referred to as the "authentication functions") using passwords and other

information (i.e. passwords, IC cards, biological information and the like; the same shall apply hereinafter), according to the nature of personal information, etc. including the confidentiality thereof (limited to those handled on information systems; the same shall apply hereinafter in this Chapter (excluding Article 55)).

Article 41.
When taking the measures mentioned in the preceding article, protection managers shall organize the provisions concerning the management of passwords and other information (including the review thereof conducted periodically or as needed) and take measures necessary to prevent passwords and other information from being read, etc.

(Access Records)
Article 42.
Protection managers shall, according to the nature of the personal information, etc. including the confidentiality thereof, record the status of access to such personal information, etc., keep the records thereof (hereinafter referred to as "access records") for a certain period, and take measures necessary to analyze Access Records on a regular basis and from time-to-time as necessary.

Article 43.
Protection managers shall take measures necessary to prevent the alteration, theft or unauthorized deletion of access records.

(Monitoring of Access Status)
Article 44.
Protection managers shall, according to the nature of (including the confidentiality and amount of) the personal information, etc., take necessary measures for the monitoring of inappropriate access to the personal information, etc. including setting up a function that displays a warning message when more than a certain amount of information that contains or may possibly contain personal information, etc. is downloaded from an information system, with periodic checking of such settings also taking place.

(Setting Up of Administrative Privileges)
Article 45.
Protection managers shall, according to the nature of the personal information, etc., including the confidentiality thereof, take necessary measures to minimize damage when privileges of authority for information system administrators are stolen, and shall take measures to prevent any internal unauthorized operation or other activities (including the minimizing of such privileges).

(Prevention of Unauthorized Access from Outside)

Article 46.

Protection managers shall take necessary measures to prevent unauthorized access from the outside to information systems handling personal information, etc. (including path control via firewall setups).

(Prevention of Leakage, etc. by Malicious Programs)

Article 47.

In order to prevent leakage, etc. of personal information, etc. by malicious programs, protection managers shall take necessary measures for the resolution of disclosed vulnerabilities in software and the prevention of infection by detected malicious programs (including keeping all installed software up-to-date).

(Handling of Personal Information, etc. on Information Systems)

Article 48.

When making reproductions or other copies of personal information, etc. to perform temporary processing of the data, academic and administrative staff shall limit the copying of personal information, etc. to the minimum necessary extent, and promptly delete any information that becomes redundant promptly after the completion of the processing. Protection managers shall perform checks with a focus on the status of implementation (such as deleted statuses) as needed according to the nature of such personal information, etc. (including the confidentiality thereof).

(Encryption)

Article 49.

According to the nature of the personal information, etc. including the confidentiality thereof, protection managers shall take the measures necessary for encryption. Based on the above, academic and administrative staff shall properly encrypt the personal information, etc. they are handling in accordance with the nature of such personal information, etc. including the confidentiality thereof.

(Restriction on Connecting Devices/Media with Recording Functions)

Article 50.

According to the nature of the personal information, etc. including the confidentiality thereof, protection managers shall take necessary measures to prevent leakage, etc. of such personal information, etc. including the restriction of connecting devices/media with recording functions such as smartphones and USB memory sticks to the information system terminals or other devices (including connecting such devices for updates).

(Limitation of Terminals)

Article 51.

Protection managers shall take necessary measures to limit the terminals that handle personal information, etc., according to the nature of such personal information, etc. including the confidentiality thereof.

(Preventing Theft of Terminals, etc.)

Article 52

Protection managers shall take necessary measures for the prevention of theft or loss of terminals including fixing terminals or locking offices.

Article 53.

Unless a protection manager deems it necessary, academic and administrative staff must not take any internal terminals to areas outside the organization or bring in any terminals from outside of the organization.

(Preventing Browsing by Third Party)

Article 54.

When using terminals, academic and administrative staff shall take necessary measures to ensure that personal information, etc. cannot be browsed by a third party, including ensuring that they log off from the information systems depending as and when necessary, depending on the conditions of use.

(Verification of Entered Information, etc.)

Article 55.

Academic and administrative staff shall, according to the importance of the personal information, etc. handled using the information systems, shall compare and verify source documents and the entered details, confirm details of such personal information, etc. before and after handling, verify the content thereof using existing retained personal information, etc.

(Backup)

Article 56.

Protection managers shall make backups and take necessary measures to store the data in a separate location according to the importance of the personal information, etc.

(Managing the Design Specifications etc. of the Information System)

Article 57.

Protection managers shall take necessary measures for the storage, reproduction, disposal and other arrangements of documentation such as the design specification of the information system and configuration diagrams relating to personal information, etc. to prevent them being known by unauthorized persons.

Chapter 8. Managing the Security of the Information System Offices, etc.

(Controlling Entrance and Exit)

Article 58.

Protection managers shall specify the persons authorized to enter an office where devices (including the main server that handles personal information, etc.) are installed or other areas (hereinafter referred to as "information system offices, etc."), and take measures including the confirmation of business, recording of instances of entrances and exits, means of identifying external entities, accompaniment of external entities by academic and administrative staff, or their monitoring by monitoring devices, restrictions on bringing in, use and removal from the premises or inspection of external electromagnetic recording media or other media. In addition, in cases where facilities to store media recording personal information, etc. are established, protection managers shall take similar measures when deemed necessary.

Article 59.

Protection managers shall, when deemed necessary, take necessary measures including installation of entrance and exit controls by specifying the doorways to the information system offices, etc., and limiting the display of its locations.

Article 60.

Protection managers shall, when deemed necessary, take measures necessary for setting up an authentication mechanism for entrance, and organizing the provisions regarding the management of passwords and other information (including the review of such conducted periodically or as needed), means to prevent passwords and other information from being read, and for conducting other arrangements in relation to the control of entrance to, and exit from the information system offices and its storage facilities.

(Control of Information System Offices, etc.)

Article 61.

In order to prevent illegal intrusion from outside parties, protection managers shall take measures that include the installation of locking units, alarm systems and monitoring devices in the information system offices, etc.

Article 62.

In preparation for disaster and other events, protection managers shall take necessary measures within the information system offices, etc. including measures for earthquake resistance, fire prevention, smoke prevention, water resistance, as well as take measures which include the securing of standby power supplies for devices (including servers) and the prevention of wiring from being damaged.

Chapter 9. Handling of Specific Personal Information, etc.

(Restrictions on the Use of Individual Numbers)

Article 63.

Protection managers shall take measures to limit the use of individual numbers to the affairs restricted in advance by the Numbering Act.

(Restrictions on Requests for Provision of Specific Personal Information, etc.)

Article 64.

Academic and administrative staff shall not request the provision of individual numbers except in cases necessary for processing affairs related to individual numbers or other cases specified by the Numbers Act.

(Restrictions on the Creation of Specific Personal Information Files)

Article 65.

Academic and administrative staff shall not create specific personal information files, except in cases necessary for processing affairs related to individual numbers or other cases specified by the Numbers Act.

(Restrictions on Collection, Storage and Provision of Specific Personal Information, etc.

Article 66.

Academic and administrative staff shall not collect, retain or provide personal information, including the Individual Numbers of others, except in cases that fall under any of the items of Article 19 of the Numbers Act.

(Clarification of Areas for Handling of Specific Personal Information etc.)

Article 67.

Protection managers shall clarify the areas where affairs for the handling of specific personal information, etc. are to be implemented and shall take physical safety management measures.

(Records of the Handling Status of Specific Personal Information Files)

Article 68.

Protection managers shall establish means for confirming the status of the handling of specific personal information files and shall record the status of the handling of said specific personal information, etc. such as the use and storage of said specific personal information, etc.

(Restrictions on the Provision of Specific Personal Information, etc.)

Article 69.

Protection managers shall not provide specific personal information, etc. except in cases where it is specifically specified by the Numbering Act.

(Outsourcing, etc.)

Article 70.

When outsourcing all or a part of Individual Numbers related affairs, protection managers shall confirm in advance whether or not the service provider will take the measures equivalent to the security control measures to be fulfilled by the University pursuant to the Numbers Act.

Article 71.

When outsourcing all or a part of affairs related to the Individual Numbers, protection managers shall conduct necessary and appropriate supervision so that the contracted party may take measures equivalent to the safety management measures to be taken by the University

Article 72.

When the service provider subcontracts all or a part of affairs related to Individual Numbers, protection managers shall determine the approval or disapproval of the subcontracting after confirming that proper security will be ensured with respect to the control of specific personal information handled in connection with affairs related to individual numbers to be outsourced. The same shall apply thereafter in the cases where the subcontractor re-subcontracts.

Article 73.

1. The provisions of Article 19, Paragraph 1, items (3) through (6), Article 22, Paragraph 2 and Articles 29 through 32 shall not apply to specific personal information retained or intended to be retained by the University. For the purpose of the application of the other provisions of these Rules, the terms listed in the middle column of the following table in the provisions listed in the left column of the same table shall be deemed to be replaced with the terms in the right column of the same table.

Provisions of these Rules whose terms are to be replaced	Terms deemed to be replaced	Terms to be replace with
Article 19, Paragraph 1, item (1)	in accordance with laws and regulations	cases based on the provisions of Article 9, paragraph 5 of the Numbers Act
Article 19, Paragraph 1, item (2)	individual	with the consent of the individual or the individual in question
Article 19, Paragraph 2	shall obtain prior consent from the individual in question when handling personal information beyond the scope of the purpose of use specified pursuant to the provisions of the preceding Article.	personal information shall not be handled beyond the scope of the purpose of use specified pursuant to the provision of the preceding Article.

2. With regards to the Individual Numbers, these Rules shall apply to the Individual Number even after the death of the individual concerned, and the person in charge of handling the affairs shall take the necessary measures.

Chapter 10. Response to Security Problems

(Incident Reporting and Measures to Prevent Recurrence)

Article 74.

When becoming aware of an incident that would become a problem in terms of security, such as cases where one becomes aware of the occurrence or sign of an occurrence of incident of leakage, etc. of personal information, etc. and where being aware of a fact or signs pointing to facts that an affairs handling officer is in breach of the provisions of related laws and regulations and rules, academic and administrative staff shall immediately report the facts thereof to or consult with the protection manager who manages such personal information, etc.

Article 75.

Protection managers shall promptly take measures necessary for the prevention of escalation of damage or restorative actions or take other arrangements, as well as report to organization senior protection managers; provided, however, that protection managers shall immediately take (or cause academic and administrative staff to take) measures that can be taken immediately to prevent escalation of the damage, with such measures including the unplugging of LAN cables of the relevant terminals (or other devices) in which unauthorized access from the outside (or inspection by a malicious program) is suspected.

Article 76.

Organization senior protection managers shall investigate the background of the occurrence of incidents, damage situations and other matters and report the facts thereof to the senior protection manager. However, any incidents deemed to be specifically serious, the protection managers shall immediately report the details thereof and other information relating to such incidents to the senior protection manager.

Article 77.

When receiving a report under the provision of the preceding Article, the senior protection manager shall promptly report the details, background, damage situation, and other information of such incidents to the President in accordance with the nature of such incidents.

Article 78.

The senior protection manager shall promptly provide the relevant ministries and agencies with information including the details, background, and damage situation of an incident in accordance with the nature and other factors relating to the incident.

Article 79.
Protection managers shall, under the supervision of the organization senior managers, analyze the causes leading to the incident and take measures necessary to prevent the recurrence thereof.

(Publication, etc.)
Article 80.
1. The senior protection manager shall, according to the nature, impact and other factors of an incident, take measures including the publication of facts and measures to prevent recurrence and responses to individuals relevant to personal information, etc. involved in such incidents.
2. The senior protection manager shall promptly provide the relevant ministries and agencies with information, which includes the details, background, and damage situation of such incidents, regarding incidents to be publicized.

Chapter 11. Implementation of Audit and Inspection

(Audits)
Article 81.
The general auditor shall perform an audit (including an external audit; the same shall apply hereinafter) on a regular basis and from time-to-time as needed with respect to the status of management of the personal information, etc. at the University, including the status of measures set forth in Chapter 2 through Chapter 10, verify the proper management of retained personal information, etc. and report the results thereof to the senior protection manager.

(Inspections)
Article 82.
1. Protection managers shall perform an inspection on a regular basis and from time-to-time as needed with regards to recoding media, processing route, method of storage and other matters of personal information, etc. at each organization or any other division, and when deemed necessary, report the result thereof to organization senior protection managers.
2. Any organization senior protection supervisor who received a report of the preceding paragraph must report the important parts of such report to the senior protection manager.

(Evaluations and Reviews)
Article 83.
The senior protection manager and organization senior protection managers shall evaluate the measures for proper management of the personal information, etc. in terms of effectiveness or other aspects based on the results of audits or inspections and other factors, and when deemed necessary, take measures including revision thereof.

Chapter 12. Cooperation with Administrative Agencies

Article 84.

The University shall properly manage the personal information held by it based on the "Basic Policy on the Protection of Personal Information" (Cabinet Decision 4 of April 2, 2004), by closely cooperating with relevant ministries and agencies.

Supplementary Provisions

These Rules shall come into force as from April 1, 2005.

Supplementary Provisions

These Rules shall come into force as from January 1, 2011.

Supplementary Provisions

These Rules shall come into force as from April 1, 2015.

Supplementary Provisions

These Rules shall come into force as from November 1, 2015.

Supplementary Provisions

These Rules shall come into force as from April 1, 2016.

Supplementary Provisions

These Rules shall come into force as from December 1, 2017.

Supplementary Provisions

These Rules shall come into force as from April 1, 2018.

Supplementary Provisions

1. These Rules shall come into force as from April 1, 2019.
2. For the purpose of the provisions of Article 4 during the date of enforcement of these Rules to March 31, 2021, the “The University of Tokyo Archives” in the same article shall be deemed to be replaced with “The University of Tokyo Archives, University-wide Centers listed in the Supplementary Provisions of the Regulations for the partial revision of the University of Tokyo Rules on Basic Organization (The University of Tokyo Rules No. 3, April 26, 2018).

Supplementary Provisions

These Rules shall come into force as from March 1, 2020.

Supplementary Provisions

These Rules shall come into force as from April 1, 2021.

Supplementary Provisions

These Rules shall come into force as from April 1, 2022.