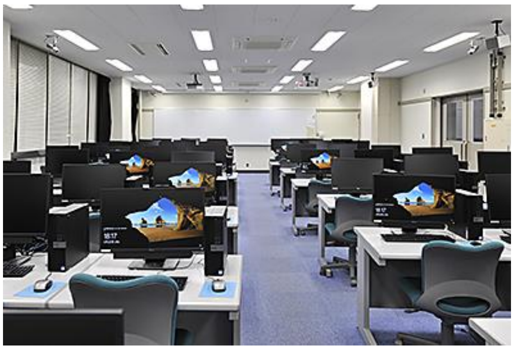
User's Guide to Zengaku and Other Computing Systems at the University of Tsukuba



Eleventh Edition (1 April 2017)

Academic Computing and Communications Center, University of Tsukuba

Introduction

This is a concise user's guide to the University of Tsukuba computing systems, such as the Zengaku Computer System (the Kyotsu Education System shared by the entire university), the On-Campus Network, and various other services provided by the Academic Computing and Communications Center (hereafter referred to as the ACCC). For detailed information, please see the ACCC website (http://www.cc.tsukuba.ac.jp/) user's guide for each of the systems, and each of the manufacturer's instruction manuals.

The services of the ACCC may only be used for the purposes of education and research at the University of Tsukuba. Some of the services are fee-based. In this user's guide, services that are subject to fees are designated as [paid service]; however, the user cannot pay by personal payment. The user needs to consult with their home room professor or instructor and follow their guidance accordingly.

Zengaku Computer System summary

1. Summary of the system

The Zengaku Computer System serves 1,100 computer terminals in on-campus satellites for student use.

Each of the computer terminals is dual-bootable with Windows and Linux. The user chooses the desired platform when the computer terminal is powered on. As NetBoot technology is used in the system, the user can work in the same environment with the same start-up image from any terminal on the system.

For the latest information on the Zengaku Computer System, see the following webpage:
http://www.u.tsukuba.ac.jp/

2. Available Satellite computer rooms

Area of Location	Satellite	Room	Number of terminals
Central Area	2D Satellite	2D201	20
		2D202	101
		2D203	
		2D204	
	2A Satellite	2A303	15
		2A304	23
	Bunshu Satellite	8B201	28
	3K Satellite	3K203	40
	3D Satellite	3D207	46
	Central Library Satellite	2F Communication room	17
		2F Reading room	66 (1)
		3F Reading room	6
		4F Reading room	6
		5F Reading room	6

Area of Location	Satellite	Room	Number of terminals
Central Area	1C Satellite	1C206	45
	1D Satellite	1D301	81
South Area	Academic Computing and Communications Center Satellite	A203	51
		A207	10
		B205	61
		B206	51
	Art and Physical Education Library Satellite	Audio-visual room	41 (1)
West Area	Medical Satellite	4A402	26
		4B212	62
	Medical Library Satellite	Computer room	42(1)
Kasuga Area	Kasuga Satellite	7C102(Lab Ⅰ)	76
		7C103(Lab Ⅱ)	28
		7C202(Lab Ⅲ)	69
	Library on Library and Information Science Satellite	1F Reading room Kasuga Learning Commons	17 (1)
Tokyo Campus	Tokyo Satellite	4F 454	20
	Otsuka Library Satellite	B1	11(1)

Notes:
(number) indicates the number of terminals for people with visual and hearing disabilities.

As a rule, the satellite computer rooms are available when they are not in use for classes. Please refer to the time tables that are posted at each satellite for details on available times.

In the ACCC Satellite, computer room users must leave the ACCC building before 22:05, as the entrance to the building closes automatically at this time.

Please also note that the satellites are not available on maintenance days. These days will be announced on the Zengaku Computer System website.

3. Password

To use the Zengaku Computer System, users are required to have a Unified Authentication Password. For eligibility, see the table below. For issuing and changing the password, see the section on the Unified Authentication System (page 4) for details.

■ Eligibility

Please refer to the following table for eligibility for the Zengaku Computer System.

Category	Remarks
Undergraduate and graduate students, Credited Auditors, Non-degree Research students, Exchange students Non-degree Research students affiliated with Int'l Student Center and trainees in the intensive Japanese program, Post-J.D. trainees	Eligible from entrance until graduation with no need of application. Zengaku Computer System ID and Unified Authentication Password are used. Zengaku Computer System ID has 8 digits, consisting of "s" and the last 7 digits of Student ID. (This ID is called "UTID-NAME" as well.)
Short-term students (e.g. short-term study program participants etc)	To be eligible to use the Zengaku Computer System, an application is required at the office of ACCC. Contact ACCC for the procedure.

4. Notes on using the Zengaku Computer System

■ Users of the Zengaku Computer System are expected to carefully read the detailed regulations and guidelines on computer systems (starting on page 12) and observe the rules. Please pay special attention to copyright infringement regulations.

■ Student ID (IC card) is required for using printers. Students who are not entitled to a Student ID are able to substitute this with the Zengaku Computer System Satellite User Card. To obtain the card, an application at the office of ACCC is required. Please contact the ACCC for the procedure.

■ Users are permitted to use the Zengaku Computer System only while they are registered with the University of Tsukuba; the system is not available after graduation or completion of graduate work. If an undergraduate student proceeds to study at the graduate level, a new Student ID as well as an account name for the Zengaku Computer System will be assigned. Users are encouraged to finish transferring necessary data and set up e-mail forwarding before graduation.

Summary of services

1. Information infrastructure-related services

ACCC offers the following services:

(1) Unified Authentication System

This system manages the ID and password of students (undergraduate and graduate) and full-time administrative staff. On the system, user authentication is based on the combination of ID and password, and the following two types of ID are used:

●Unified Authentication ID（UTID-13）

The Unified Authentication ID consists of a 13 digit number shown on the back of Student ID card. This ID is also written as "UTID-13".

●Unified Authentication User Account（UTID-NAME）

The Unified Authentication User Account is the user name assigned to each user, and for students, it is "s" followed by the last 7 digits of Student ID. This ID is also written as "UTID-NAME".

While which of the two types of ID is used depends on the system, some systems accept both.

Users can view registered personal information and change their passwords on the website of Unified Authentication System. If students who are not entitled to a Student ID card need a Unified Authentication ID, they need to consult with the office of ACCC.

The following table shows the systems where the Unified Authentication is required:

Name of the system	ID (Student)
Unified Authentication System	UTID-13
On-Campus Access Points (Zengaku Information Outlet and Network System, On-Campus Wi-Fi System, VPN connection system)	UTID-13
Zengaku Computer System (including @u and @s emails)	UTID-NAME
Center for Education of Global Communication CALL System	
College of Information Sciences Educational System	
Tsukuba University Library Information Processing Systems (TULIPS)	UTID-13 or UTID-NAME
E- Learning Management System (manaba)	
Tsukuba Web-based Information Network System(TWINS)	Student ID (9 digit number)

Please note that eligibility varies depending on the system. Thus registration with the Unified Authentication System does not necessarily ensure that the user will be eligible to use any particular system. The Unified Authentication System also registers the various IDs and passwords used on each of the systems. Contact each system's administrator for details.

■ Registered users and initial password

The following users are registered by default (no need for an application).

Category	Initial Password
Undergraduate and graduate students, Credited Auditors, Non-degree Research students, Exchange students Non-degree Research students affiliated with Int'l Student Center and trainees in the intensive Japanese program, Post-J.D. trainees	Initial password offered during the enrollment proceedures

■ Reviewing personal information

Users can review their registered personal information on the Unified Authentication System Web Server (https://account.tsukuba.ac.jp/). Go to the "Review your information" page and enter your Unified Authentication ID (UTID-13) and password.

■ Changing password

Users can change their password on the Unified Authentication System Web Server (https://account.tsukuba.ac.jp/). Note that it might take some time before the change takes effect. For security reasons, it is not advisable to leave the initial password unchanged. Users are urged to change their password on a regular basis.

■ Forgotten password

Users can obtain a new Unified Authentication password in case they forget their password. Bring your Student ID card and come to one of the offices below:

・ACCC, Office (Phone: 029-853-2452)
・Kasuga Satellite, Office
・Central Library, Reference Desk
・Art and Physical Education Library, Reference Desk
・Medical Library, Main Counter
・Library on Library and Information Science, Main Counter
・Otsuka Library,　Service Counter

☆ Inquiries about the Unified Authentication System:
Write to: ldap-staff@cc.tsukuba.ac.jp

(2) E-mail and Publishing Websites

a) E-mail

Zengaku Computer System users are able to use email on this system.
The email address is:

○Students enrolled in or after April 2017 ⇒ "s + last 7 digits of the Student ID Number @s.tsukuba.ac.jp"

○Students enrolled in or before March 2017 ⇒ "s + last 7 digits of the Student ID Number @s.tsukuba.ac.jp", and "s + last 7 digits of the Student ID Number @u.tsukuba.ac.jp" (both addresses are available)

○Others (Faculty, etc.) ⇒ "Zengaku Computer System ID @u.tsukuba.ac.jp"

You can also use the web mailer for sending and receiving email:
■@s.tsukuba.ac.jp ⇒ https://cloudmail.u.tsukuba.ac.jp
■@u.tsukuba.ac.jp ⇒ https://wmail.u.tsukuba.ac.jp

The University of Tsukuba sends official and important messages to this e-mail address. Please check your mail box regularly. Moreover, you can redirect e-mails from this e-mail address to another e-mail address.

b) Publishing websites

Zengaku Computer System users are able to publish websites using the server computer (www.u.tsukuba.ac.jp). Before publishing a web site, the user is required to carefully read and agree with the guidelines on the Web Server Application page on the Zengaku Computer System web site (http://www.u.tsukuba.ac.jp/). They will be able to publish it after registering from “Publishing Web Content” in ”Personal Setup” on the same website.

(3) Connecting to the On-Campus Network

At the University of Tsukuba, graduate schools, doctoral and master’s programs have formed a Sub-network Administration Committee (SAC) to administer the information outlet systems that are installed at laboratories. For information on how to set up personal computer terminals to get connected with each of the information outlet systems, ask the instructors or professors of each laboratory, or SAC for details. For more information on SAC, please refer to the chart of the Organization for Information Infrastructure (OII) on the OII website (http://www.oii.tsukuba.ac.jp/). (Use the left-side menu as follows:「情報セキュリティ関係 (Information Security)」 >「情報セキュリティ組織・体制 (Information Security Organization Chart)」>「12. 全学及び部局等の情報セキュリティ関係委員会等 (Information Security Committee Chart)」

ACCC also operates Access Points to allow personal computer terminals to be connected with the on-campus network. Personal terminals such as laptop computers can be connected to the on-campus network by connecting with the information outlets in lecture rooms, or On-Campus Wi-Fi Network Access Points throughout the campus. Also, from off-campus locations, using the VPN Server through the internet enables the users to be virtually connected with the campus network.

To be able to utilize these connection services, users must have a Unified Authentication ID (UTID-13) and a password. If you have any problems with your ID (UTID-13), please contact the ACCC.

For information on the location and the method of each connection service, please obtain the latest information from the website on Access Point services at the following URL:

http://www.cc.tsukuba.ac.jp/wp_e/service/notice

The above website deals with both off-campus and on-campus terminals (Zengaku Computer System terminals).

☆ Inquiries about Access Points

Fill in: http://www.cc.tsukuba.ac.jp/wp_e/contact

a) Zengaku Information Outlet and Network System

Information outlets in the lecture rooms function as the Zengaku Information Outlet and Network System. The following table shows locations of information outlets.

Area	Location
North Area	(none)
Central Area	Lecture rooms at 1E Building, 2C Building, 2D Building, 3A Building and 3B Building, Lecture Hall at Laboratory of Advanced Research A, Lecture Hall at Laboratory of Advanced Research B
South Area	Lecture rooms at 5C Building, 30th Anniversary Hall, Lecture Hall at Laboratory of Advanced Research D
West Area	(none)
Kasuga Area	Rooms in International Student Hall, Union of Library and Information-media Studios, Welfare Facilities, Lecture rooms at 7A Building, Kasuga Auditorium
Otsuka Area	Lecture rooms, Lounges, Student Hall at Bunkyo School Building

b) On-Campus Wi-Fi System

Users who have personal laptop computers equipped with Wi-Fi connectivity can get connected with the on-campus network system at almost all the schools and college's lecture rooms and cafeterias.

Please note that Room 207 at the ACCC building, diagonally in front of the ACCC office, is open for users of On-Campus Wi-Fi System, inviting questions about how to get connected on the system. General questions, such as how to use one's own computer, are not accepted. Please be aware that Room 207 is an experimental operation, therefore the service could be terminated without prior notice.

Notes:

There are numerous Wi-Fi access points on campus, not all of which are administered by ACCC. For these non-ACCC Wi-Fi access points, users need to make inquiries with each of the administrators.

c) VPN connection system

When the user attempts to connect a personal computer from home or from an off-campus location with the "university-only" (or accessible only from on-campus network) websites, generally the web pages cannot be viewed. Furthermore, a personally owned computer may not be allowed to enter all of the numerous servers on the university network because there is a firewall that prevents unauthorized computer access from off-campus locations.

ACCC operates a VPN connection service for users to connect to the university network from an off-campus location through the internet by virtually connecting them from within the university network.

For the instructions on how to use the VPN server, see the following website:
`http://www.cc.tsukuba.ac.jp/wp_e/service/vpn`

■ Note on using the Access Point Connections

When using the Access Point Connections, users should observe the Detailed Regulations for Access Point Users at the University of Tsukuba Academic Computing and Communications Center.
`http://www.cc.tsukuba.ac.jp/c_publication/kisoku/access.pdf`

- Use of peer-to-peer file sharing software (such as Xunlei, BitTorrent, µTorrent, Limewire, Cabos, WinMX, Share, Winny, etc.) is prohibited. If students wish to use it on campus for legitimate purposes, they are obligated to apply to the Network Management Committee after consulting with their instructor.
- File-sharing functions on operating systems enable other users to view files on your computer. They should be used with care.

- A firewall system is set up for the safety and security of the access point users in order to screen and detect virus-infected computers or inadequately used terminals. (*1)

- Users of Access Point Connections need a Unified Authentication ID (UTID-13) and password. There is no special fee charged for using Access Point Connections; however, the user needs to have a computer terminal equipped with the network interface, and cover the communication fee that connects the user's personal computer to the internet and the ISP connection fee to connect to the VPN connection system.

Note:

(*1) The system records information regarding the sender, the receiver, the time the communication began, the duration of the communication, and the volume of information transmitted, and utilizes the information to detect unauthorized use. The content of communication, however, is never recorded.

d) Computer time synchronization service

ACCC operates a Stratum1 NTP server to provide accurate timing reference, receiving precise time information from a GPS satellite system.

For synchronization of the internal clock of computer devices connected to the on-campus network using Stratum1, ACCC operates a Stratum 2 NTP server for users to synchronize clocks as follows:
Host name: `timeserver.cc.tsukuba.ac.jp`

e) DNS cache service

ACCC offers a DNS cache service for network devices connected at the University of Tsukuba to enable name retrieval on the internet.
IP address: 130.158.68.25
130.158.68.26

Please note that if the user's setting is "Automatically acquire DNS server address" on the ACCC Access Point connection, the above is set automatically as the DNS server.

f) Software license agreements at the University of Tsukuba

The University of Tsukuba has made license agreements with a number of computer software companies to make applications (such as a site license for the statistical software SPSS) available to teachers, students and administrative staff.

Students and teachers are already entitled to academic edition software discounts when purchasing computer software. However, Tsukuba University teachers and students can obtain a further discount by using one of these licensing agreements that the university has made with software companies.

For further information on the licensing and discount agreements, see the following website for the latest information on terms and conditions.

http://www.cc.tsukuba.ac.jp/wp_e/service/software-license/

2. Office of Educational Cloud Services

(1) Learning Management System

■ Outline

The University of Tsukuba has introduced manaba as a learning management system. The learning management system is a system that, through the use of a web browser, will facilitate a variety of functions including the distribution of lecture materials, the submission of reports, and attendance checks. Classes utilizing the learning management system will be able to register courses on the system. This will result in the creation of a "course page" (webpage) which will be accessible for the class. (For more details, please follow the instructions given during the class).

The following functions will be available on the course page.

- Students will be able to browse the course outline and lecture materials uploaded by the instructor.
- Notifications from the instructor will be posted under "course news." Students will be automatically informed by email when notifications are posted.
- Assignments and small tests can be submitted.
- Attendance can be taken with the learning management system.

Please follow the directions given by the instructor in charge as to which functions to use.

■ How to login

Basically, anyone enrolled at the University of Tsukuba can use the system. In order to login you must have a unified authentication ID and password. Access the login page at https://manaba.tsukuba.ac.jp/ and enter your unified authentication ID (13 digits) into the user name box, and your unified authentication password into the password box.

■ Contact information, user guides and other documentation

User guides and other documents are posted on the Office of Educational Cloud website, http://www.ecloud.tsukuba.ac.jp/. Other important notices, such as system outages, are also posted to the website as needed.

Additionally, a help desk has been setup in the Office of Educational Cloud and staffs are available to answer questions as needed. Please contact us if you are having any troubles using the system.

- TEL: 029-853-6892 (9:30-12:00,13:15-17:00, excluding Saturday, Sunday and public holidays)
- Email: support-manaba@ecloud.tsukuba.ac.jp

(2) Remote Lecture & Automatic Recording System

This system has been introduced to record classes and to offer remote lectures in a user friendly way. Devices in classrooms automatically boot up and start remote lecture operation. Recorded videos can be distributed to students via manaba. For more information, visit the "Remote Lecture & Automatic Recording System" webpage in the Office of Educational Cloud website:

http://www.ecloud.tsukuba.ac.jp/en/vls

(3) Multimedia service

With regard to media production, editing, storage and distribution, the Office of Educational Cloud offers the services listed below. If you are interested, please check the Media Services page (http://www.ecloud.tsukuba.ac.jp/media/) accessible from the Office of Educational Cloud website.

1. Video production, broadcasting, editing (fee-based)

   Professional quality video by technically qualified staff including video planning, filming and editing.

2. Video distribution service (fee-based)

   We will act as agents and deliver your video over the Internet.

3. Video/audio-based teaching material and document production services (fee-based)

   We can assist with the creation of video/audio-based teaching materials. Due to technical innovation many types of video and audio mediums exists. We are able to support the organization and creation of on-campus teaching materials and documents with a wide variety of formats, including those from the past up to the latest types. Additionally, we are able to provide production facilities with a studio, recording room, and editing system.

4. Poster printing and large-format copying service (fee based)

   With our large-format inkjet printer (Canon iPF8300S) we are able to print posters, horizontal banners, and billboards. Copying is also possible in combination with our 36-inch manuscript movable full color scanner.

Contact Information

For further information please access the Academic Computing and Communications Center website (http://www.cc.tsukuba.ac.jp/) and the Office of Educational Cloud website http://www.ecloud.tsukuba.ac.jp/).

1) Clerical matters such as user registration, appointments, billing, user guidelines application, and password settings
   ・Center Office (reception desk): 029-853-2452
      ○ Business hours: Weekdays, 8:30-12:15 and 13:15-17:15
2) Technical matters such as system utilization, system failures
   ・Operator: 029-853-2455, 2457
3) Document inquiries and application forwarding

   〒305-8577
   1-1-1 Tennodai Tsukuba, Ibaraki Prefecture
   Office, Academic Computing and Communications Center, University of Tsukuba,
   Fax:029-853-2478

4) Educational cloud related inquiries
   ・Office: 029-853-6891
   ・Learning Management System Help Desk: Inquiries by phone is closed for a while. Accepted only by email: support-manaba@ecloud.tsukuba.ac.jp.
   ・Remote Lecture/Automatic Recording Lecture System: 029-853-2440
   ・Video Production, Audio/Video: 029-853-2424
   ・Photo Archives, Large-format Copying/Poster Printing: 029-853-2445
   ・Video Distribution: 029-853-6893

Guidelines

Note:

These documents were originally written in Japanese. If there are any differences between the Japanese document and the English document, the Japanese version shall take precedence.

1. Regulations on Use of Information Systems at the University of Tsukuba

Corporate Regulations No. 55
April 1, 2013

(Original title: 国立大学法人筑波大学情報システムの利用に関する規程　法人規程第 55 号)

(Purpose)

Article 1:　Based on the provisions of Article 90 of the basic rules on organization and administration at the University of Tsukuba (hereafter referred to as the University), Corporate Regulations No.1 of 2004, this regulation shall provide for necessary matters concerning the use of information systems (information systems which the University holds or hereafter referred to as Information System).

(General rule of use)

Article 2:　The Information System shall only be used when it is found that such use is necessary from the view point of education, research and social contribution of the University, administration of the University as well as education and research for inter-university purposes.

(Scope of users)

Article 3:　Those who are eligible to use the Information System fall under one of the following categories.

(1) Officers and employees of the University

(2) Students (including Credited Auditors, Non-degree Research Students, Exchange Students, Exchange Research Students, Intensive Japanese Language Course Students) of the University

(3) Professors Emeritus of the University of Tsukuba, University of Tsukuba College of Nursing and Medical Technology, University of Library and Information Science, and Tokyo University of Education that were installed pursuant to the provision of the former Act for Establishment of National Universities (before the abolition, pursuant to the provision of Article 2, of the act on development of legal systems in enforcing national university corporation and such (Act No. 117 of 2003), of Act for Establishment of National Universities (Act No. 150 of 1949))

(4) Researchers prescribed in Article 2 of the regulations on receiving researchers at the University of Tsukuba (Corporate Regulations No. 53 of 2005)

(5) Collaborative Researchers from such organizations as corporations, as prescribed in Article 9 of the regulations on collaborative research at the University of Tsukuba (Corporate Regulations No. 45)

(6) Teachers, students or equivalent from other universities (also includes colleges), technical colleges, and inter-university research organizations

(7) Those who the Director of the Organization for Information Infrastructure finds necessary

(8) Those who the directors of each organization that manages the respective information systems (hereafter referred to as Information System Administrator) find necessary

(User application and approval)

Article 4:　As a general rule, the Information System Administrator of each of the systems shall have those who intend to use the Information System make applications in such a way that the Information System Administrator specifies.

2.　The Information System Administrator shall have those who were approved to use the Information System as per the previous paragraph (hereafter referred to as Users) familiarize themselves with the necessary matters of the use of the Information System.

(Fees)

Article 5:　The Information System Administrators may request Users to incur costs as required.

(Report of usage)

Article 6: The Information System Administrators may request reports from Users on matters pertaining to usage of the Information System as required.

(User's responsibility)
Article 7: Users must observe the regulations on using the Information System, as well as follow the instructions of the Information System Administrator.

(Notification of change)
Article 8: Users must promptly report to the Information System Administrator when there is a change in information that has been previously submitted.

(Report of accident or failure)
Article 9: Users must immediately report to the relevant Information System Administrator when they find a failure in the Information System.

(Cooperation to resolve problems)
Article 10: Users must cooperate in resolving the problems in the Information System when a failure occurs.

(Rescission of user approval)
Article 11: When a User violates these regulations or other rules, or brings about serious problems in the operation of the System, the Information System Administrator may rescind the approval of or suspend the User.

(Compensation for damages)
Article 12: When a User intentionally or by gross negligence causes damage or loss to the facilities or the like, the President of the University may make the User compensate for the damage.

(Detailed regulations)
Article 13: In addition to what is provided for in these Corporate Regulations, other necessary matters in the use of respective Information Systems shall be prescribed by the departmental regulations approved by the directors of departments, on-campus joint educational and research facilities (except for specific directors carrying out administrative operations for the Doctoral Programs at Graduate Schools), and inter-collegial facilities (hereafter referred to as Directors).

2. Directors shall provide the President of the University with the departmental regulations set forth in the preceding paragraph, and report promptly in case of revision or abolition of such regulations.

(Miscellaneous provision)
Article 14: In addition to what is provided for in these Corporate Regulations, necessary matters pertaining to the use of the Information System shall be provided separately.

Supplementary provisions
These Corporate Regulations are in effect as of April 1, 2013

2. Guidelines for the Use of Information Systems at the University of Tsukuba

September 26, 2008
Information Infrastructure Committee

(Original title: 筑波大学における情報システム利用のガイドライン　情報環境委員会決定)

1. Purpose of the guidelines

The following guidelines refer to the rules with which users of the information systems need to comply with at the University of Tsukuba.

2. Framework of the guidelines

The guidelines consist of the following 5 main areas. Other than these, Guidelines for Releasing Information on the Web have also been established.

The five items are as follows:

Guidelines for the use of computers
Guidelines for computer security
Guidelines for password security
Guidelines for the use of e-mails
Guidelines for web browsing software

3. Guidelines for the Use of Computers

3.1 User ID

Users must not use any ID to which they are not assigned.

3.2 Password

The user must set a password that cannot easily be inferred by others, and securely control it.

3.3 Prohibition on unauthorized access

The user must not attempt or engage in unauthorized access to other information systems.

3.4 Clear indication of identity when transmitting information

Users must clearly indicate their name and affiliation when sending personal e-mail or transmitting information on the internet in order to make clear where the responsibility lies. False identity or anonymity is, as a rule, not permitted.

Releasing information on the internet refers to the following operations:

- Sending posts to mailing lists
- Releasing information on web page forms
- Sending posts to newsgroups
- Sending messages on the remote meeting system
- Sending posts on message boards
- Any other similar act pertaining to the above

3.5 Web contents policy

Information released through the internet shall, in principle, concern research or educational activities. The following activities are not allowed:

(a) Related to criminal and civil laws and regulations
- For the purpose of damaging the reputation of others
- Obscenity
- Infringement of copyright
- Infringement of privacy or image rights
- All other violations of laws and regulations

(b) Related to university regulations
- Commercial activities
- Activities concerning specific political parties or religious groups
- Damaging the reputation of and demeaning the University of Tsukuba
- Campaign activities as described in Public Office Election Law
- All other violations of university regulations

3.6 Use of computer facilities

The user must not take any actions that could possibly damage the facilities such as the computer terminals.

3.7 Net manners

The user must not disturb other users when using the network.

3.8 Network bandwidth

The user must not engage in activities that significantly occupy the bandwidth of the network.

3.9 Off campus access to the university network

The user must comply with the following rules when connecting to the university network from off-campus networks, except for the web services that are open to the public:

(a) The user must pay utmost attention in using authentication information (such as passwords and secret keys) so they will not be leaked. In case authentication information is leaked or there is a possibility of a leak taking place, the user must report to the system administrator of the university network and follow his/her instructions.

(b) The user must not attempt to connect with the university network from terminals where security is not guaranteed (such as at internet cafes).

3.10 Use of communal terminals

The user, in using the computer terminals in the computer room and shared space, must comply with the following rules:

(a) Lock the computer in the case of temporarily leaving the room while operating a terminal.

(b) Do not leave the door or windows of the computer room open. Do not change the temperature setting on the air conditioner in the room.

(c) Turn off the computer equipment after use. However this does not apply if the system administrator specifically instructed not to do so.

(d) Avoid wasting paper by not making unnecessary prints.

3.11 Installing application software

The user must comply with the following rules when installing application software:

(a) Do not install nor use P2P file-swapping software.

(b) Do not install nor use software that does not fall in line with the purpose of supporting education or research.

(c) Follow the requirements when installing and running the application.

(d) Before installing new software, always check for malware, such as viruses or spyware, using virus checking software.

(e) Do not install nor use programs of unknown origin.

3.12 Use of external media

The user must comply with the following rules when using external media such as CD-ROMs, floppy disks, and USB flash memory drives:

(a) Do not leave the external media unattended that contains the user's files.

(b) Do not use unattended external media or media whose origins are unknown on the university computers. Report the above to the system administrator if you find such media.

(c) In case the used external media are to be handed over or disposed of, completely erase the data using data erasing tools or physically destroy the media so the data cannot be restored.

3.13 Reporting obligation

The user must report promptly to the system administrator when the following are found:

(a) Vulnerabilities or problems in operating systems or applications on the computer terminals, or host computer and network equipment.

(b) Web content that might infringe copyright, classified material, or personal information on the university host computer.

(c) Web content on off-campus host computers that carries without prior consent classified material of the university, personal information of the faculty members, or content to which the university possesses the rights.

4. Guidelines for Computer Security

4.1 Virus protection

The computer terminal administrator shall check to prevent malware such as viruses and worms, and must comply with the following rules:

(a) Be aware of the vulnerabilities of the operating systems and software, and promptly make modifications to fix problems.

(b) Have the computer installed with anti-virus software and always renew the virus information database.

4.2 Installation and use of applications

The computer terminal administrator, when installing and using applications, must comply with the rules in 3.9 as well as the following rules. However, this shall not apply in cases for the purpose of or in support of education and research, for which the system administrator gives permission.

(a) Do not install or use software that could bring pressure on network bandwidth.

(b) Do not install or use applications that intercept information on packets sent out other than one's own terminal (packet sniffing).

(c) Do not install or use any other applications that infringe university regulations of network use.

4.3 Proper management of computer terminals

The computer terminal administrator must comply with the following rules:

(a) Do not alter the computer terminal settings in such a way that other people can use it without authentication. If the computer does not have an authentication function, set it up in a way that only authorized persons can use it.

(b) Set up the terminals to prevent the general public from having access to the university computer via internet.

(c) Do not allow non-account holders to use the university computers, except where it is needed for educational or research-related needs with the administrator's specific permission.

(d) For desktop terminals, lock up the facility so non-account holders cannot physically have access to it, and use wire-locks to prevent theft where needed.

(e) For portable terminals, do not leave them unattended even for a short time, and keep them in a lockable place.

(f) Set the BIOS terminal so it cannot be started up by unauthorized persons using CD-ROM or any external media, and also set a password.

(g) When a computer terminal is to be disposed of or handed over, completely erase hard drives and nonvolatile memory using appropriate software or physically destroy them, so the classified information and other vital information will not remain.

4.4 Means to cope with computer viruses

When the terminal is infected with computer viruses or virus-infection is suspected, the computer terminal administrator must remove the affected terminals from the network to prevent the spread of the viruses, contact, report and follow the instruction of the technical personnel of the department. All the network cables, wireless LAN cards, wireless LAN adaptors with USB keys must be removed from the network. If the computer terminals have built-in wireless LAN adaptors, the wireless LAN of the computer must be disabled.

5. Guidelines for password security

5.1 Changing initial password

The users must promptly change the initial password into one of their own once their account has been issued. Do not keep using the initial password when using the university information system.

5.2 Password policy

The user must set a password that meets all the conditions described below:

- Minimum length is 6 characters
- Include one letter from each of the following four categories
  - (a) upper-case letters (A-Z)
  - (b) lower-case letters (a-z)
  - (c) one or more numerical digits (0-9)
  - (d) special characters the operating system allows you to use
- Do not set passwords that can easily be inferred as follows:
  - Letters that can be deduced from the user's account information (name, user ID, etc.)
  - Anagram of the above mentioned letters or letters with numbers or special characters
  - Words found in a dictionary
  - Name of prominent figures

5.3 Password security

The user must securely control one's password. Do not write it down nor post a memo onto a computer terminal. The user must not let a third party know one's own password, and must pay utmost attention not to carelessly let others know the password.

5.4 Ban on access to university network from off-campus publicly shared terminals

Because there is a higher risk of the password and account information being stolen, do not try accessing the university network from off campus terminals used by the general public, such as internet cafes.

5.5 Changing password

The users must change their password when the account issuer (the director of the Academic Computing and Communications
Center for on-campus accounts, system administrator for each individual system) urges them to. The new password must not appear similar to the original one.

5.6 Obligation of password accident reports

The user must promptly report to the account issuer in case of a third party using one's password or the possible danger of it.

6. Guidelines for the use of e-mail

6.1 E-mail ID and e-mail address

(a) The user must not use an e-mail ID (ID for logging-in to e-mail server hereafter referred to as login ID) and/or an e-mail address that was issued to others.

(b) The user must not share a login ID and/or an e-mail address.

(c) The user must report to the technical personnel of the e-mail system department when one does not need to use e-mail any longer.

(d) The user must consult with the technical personnel of the e-mail system department for special permission or set-up when login IDs and e-mail addresses given for users with specific services, job titles or departments need to be shared by multiple people within the section, or when job responsibility was taken over by a third party.

6.2 Suspicious e-mail policy

(a) The user, unless absolutely necessary, must not open suspicious e-mails that appear to have been sent from unknown or unreliable sources.

(b) The user must not open suspicious e-mail attachments unless absolutely necessary.

6.3 Sending e-mail

(a) Always check to see if the correct e-mail address was entered.

(b) Always check for viruses when attaching files to e-mail.

(c) In the case of sending attachment files that contain confidential information, consider setting passwords on the attached file.

6.4 Contents of the e-mail

The user must not transmit e-mails that fall under the following categories:

- E-mails that infringe on confidentiality
- E-mails that infringe intellectual property rights, copyright, trademark rights, image rights, and licensing rights
- E-mails that are sexually harassing or infringe on human rights
- E-mails that contain rude descriptions and defamation of people
- E-mails that contain pyramid schemes
- E-mails that contain threats, personal money-making schemes and offers

6.5 Configure e-mail software

(a) As a rule, the user must not send e-mails in HTML format. This is to reduce security vulnerabilities for the receiver.

(b) The user must set the e-mail software to use text format (rich text format included). As a rule, the sender should not use the HTML format setting in order to avoid accessing fraudulent homepages and malicious scripts.

(c) The user must not use the preview function on the e-mail software for HTML formatted e-mails.

6.6 SPAM (junk mail)

(a) The user shall not disclose one's e-mail address unless absolutely necessary.

(b) The user, when disclosing one's e-mail address through the internet, must strive to exercise one's ingenuity, so the e-mail address cannot be automatically acquired. Some ideas include: paste the e-mail address in the form of image information, use double-byte characters on purpose, and insert unnecessary letters before and after the e-mail address.

(c) The user, when receiving unwanted mails, is encouraged to ignore them. Replying to the sender might result in confirming the e-mail address in use, thus resulting in further junk mail.

6.7 Netiquette

(a) Do not take part in sending or forwarding chain mail (the type of mail that urges the receiver to send multiple copies to other people).

(b) Do not send spam messages (e-mails that are sent at random, such as commercial direct mail) or junk mail (e-mail messages that contain useless pieces of information).

(c) Always put titles on the e-mail messages. The titles should be succinct and relevant in describing the contents of the message.

(d) Avoid using slang and abbreviated expressions that are not known to the public.

(e) Avoid using non-standard characters (Japanese characters that will not be shown correctly depending on the operating system, such as Macintosh).

(f) When writing e-mail, begin a new line after 30 to 35 characters.

(g) Notice the difference between To: and CC: in the address field in sending e-mail. To: should be used when one expects a reply from the receiver of the message.

7. Guidelines for web browsing software

7.1 Purpose of web browser use

The user must understand that the information system of this university is provided for the purpose of promotion of education and research, and performing jobs and its supporting duties, thus access to websites should be within the scope of necessity.

7.2 Web browsing policy

(a) The user must understand that by browsing any given website, the university domain name and IP address will remain as a record on the server of the website.

(b) Do not offend public order and morals by improper messages or use of the internet. Even a simple message on a bulletin board could leave a negative impression regarding the university or people associated with the university.

(c) In web searches, do not browse the results of the search without careful consideration, as it could include links to harmful websites.

(d) Do not carelessly click on links even if it is a well-known site, as there are numerous web links that try to direct the user to fraudulent sites or make the user download malicious software.

(e) While browsing web pages, do not download software when there is an obscure security warning sign that urges the user to start downloading. There are high possibilities of downloading viruses and malicious software from those sites.

(f) The user must be aware that reloading the same website repeatedly in a short time period could be regarded as a denial-of-service attack (an explicit attempt by attackers to prevent legitimate users of a service from using that service). This could cause blockage of access from the relevant domain or IP address. Other examples such as downloading a large quantity of on-line journals at the same time could result in the same access blockage problem.

(g) Do not carelessly click on the link embedded in HTML formatted mails. Those links could direct the user to fraudulent sites, such as one-click fraud sites or fake websites where they would attempt phishing. Phishing is directing the users to enter a fake website whose appearance is almost identical to the legitimate one, attempting to steal one's authentication information such as ID or passwords. It is typically carried out from links in HTML formatted mails.

7.3 Sending information to the website (entering information on forms, uploading files, etc.)

(a) In sending important information, always use a secure communication protocol such as SSL/TLS. Also check to make sure of the certificate's authenticity.

(b) In browsing websites, enter the URL directly. Using a relay site when entering data could lead to the danger of data rip-off or cross-site scripting. Cross-site scripting is a type of attack targeting the viewers of the website where the authenticity certification is relatively low. After going through a malicious site, when the user enters sensitive data, it would allow code injection called script into the data. The injected script would be sent back to the browser together with the user's input data on the server where the data is not checked. The script will never be shown on the browser screen, but on the browser where script performing is not limited, it will be carried out and important information could be stolen.
(Description from the IPA security center:
http://www.ipa.go.jp/security/awareness/vendor/programmingv1/a01_02.html)

7.4 Malicious programs

When the computer terminal is infected by a malicious program by downloading and opening a file or an infection is suspected, the computer user must remove the terminal from the network by removing the LAN cables. Afterwards, the user must contact, report and follow the instructions of the technical personnel of the department.

3. Detailed Regulations for the Use of Zengaku Computer Systems (General Education Systems)

September 26, 2008
Information Infrastructure Committee
(March 2, 2014 Modified)

(Original title: 全学計算機システム(共通教育システム)の利用に関する細則　情報環境委員会決定)

(Purpose)
Article 1: The following detailed regulations shall provide for necessary matters concerning the use of Zengaku Computer Systems (hereafter referred to as the General Education Systems) managed and operated by the Academic Computing and Communications Center (hereafter referred to as the Center) that consists of the Organization for Information Infrastructure at the University of Tsukuba based on Article 9 of the Detailed Regulations on Setting Up the Zengaku Computer System.

(Qualified users)
Article 2: Eligible users fall into one of the following categories:

1. Students at the University of Tsukuba
2. Faculty or administrative members of the University of Tsukuba
3. Postgraduate students, part-time students who are taking classes or seminars, special auditing students, special researchers, Japanese language students, researching workers, emeritus professors and part-time lecturers who apply for and are granted the use of the General Education System by the director of the Academic Computing and Communications Center (hereafter referred to as the Director).

(Application)
Article 3: Applicants for the General Education Systems must submit the prescribed application form to the Director. However, this does not apply to full-time students or faculty members.

(Approval)
Article 4: 1. The Director shall approve applications referred to in the preceding paragraph when it is found appropriate.
2. The Director shall familiarize those who are granted access (hereafter referred to as the user) with the necessary information for using the General Education Systems.

(Scope of system use)
Article 5: The Scope of the use of the General Education Systems shall fall under one of the following categories:

1. Education and research
2. Educational purposes of the users
3. Other purposes which the Director has specifically approved

(IC card)
Article 6: The user, in using the IC card which was issued for entering the satellite rooms (hereafter referred to as IC card), must comply with the following rules:

1. The user must not use the IC card other than for the purposes described in the previous paragraph.
2. The user must not allow a third party to use one's IC card or use an IC card issued to another person.
3. The user must use proper IC card security, avoiding loss or theft of the card.
4. The user must immediately report to the Director in case the IC card was used by a third party.

(Reissue of IC card)
Article 7: In case of loss or theft, the user shall apply for reissue of an IC card to the Director and pay the cost of reissue.

(Facilities and equipment use)
Article 8: The user can make use of the facilities and equipment of the Center within the scope of the use, except for the cases specified in the regulations.

(Obligation to report on usage change)
Article 9: 1. The user must report to the Director without delay in case the user does not need to use the General Education Systems anymore.
2. The user must report to the Director without delay in case there was a change in the items that were approved pursuant to the provision of Article 4.

(Obligation to report on usage)
Article 10: The user must report on the usage of the General Education Systems when asked by the Director.

(Adherence to rules)
Article 11: The user must adhere to the detailed regulations and other related rules of the university in using the General Education Systems, as well as following the instructions

of the Director.

(Prohibitions)

Article 12: The user, in using the General Education Systems, must not engage in the following activities in order to ensure and retain informational security.

1. Using the General Education Systems other than for purposes described in the scope of use
2. Transmitting information that falls under discrimination, defamation, insult or harassment
3. Transmitting information that infringes on the privacy of personal data
4. Transmitting information that infringes on confidentiality
5. Transmitting information that infringes property rights such as author's copyright
6. Infringing of privacy of communication
7. Using the system for business or profit
8. Monitoring communication on the network or acquiring information from the information processing equipment without permission or due cause
9. Any act contrary to access control as defined in the Unauthorized Computer Access Law
10. Any act including those within the scope of usage that overloads and prevents smooth operation of the General Education Systems
11. Transmitting information subject to criminal penalty or calls for civil liability such as compensation for damages
12. Changing set-ups or installed software without permission of the Director
13. All other acts that contribute to the acts described above

(Approval revocation)

Article 13: The Director has the discretion to suspend or terminate the approval of the user, if the user violated these regulations or caused a serious breakdown in the General Education Systems.

(Compensation for damages)

Article 14: If the user, approved for the General Education Systems use, intentionally or by gross negligence causes damage or loss to the facilities, the user must compensate for damages.

(Miscellaneous provision)

Article 15: Other than the above-mentioned detailed regulations, all the necessary rules shall be specified separately.

Additional note

The Detailed Regulations for the use of Zengaku Computer Systems (General Education Systems) are in force as of April 1, 2009.

Additional note

The Detailed Regulations for the use of Zengaku Computer Systems (General Education Systems) are in force as of March 2, 2012.

4. Guidelines for Releasing Information on the Web at the University of Tsukuba

September 26, 2008
Information Infrastructure Committee

(Original title: 筑波大学におけるウェブ公開ガイドライン　情報環境委員会決定)

1. Purpose

It is indispensable to release information on the internet from the University of Tsukuba. However if the information released on the web pages or message boards brings about infringement of rights, it could result in damage for the university by lowered efficiency (having to deal with the troubles created) or it could leave the public with a negative image of the university. To lessen such risks and protect informational assets, the following guidelines shall provide for necessary matters concerning the user to release information contents on the web accurately, safely, and securely.

2. Users

The following guidelines apply to all the users who release information onto web pages through the university information systems. Caution should be exercised in that the responsibilities in web contents lie with the university even when it is out-sourced to external contractors.

3. General rules

The internet users on the university network systems who are releasing information must abide by both civil and criminal
laws and regulations, as well as regulations on the use of the university network, SINET (Science Information Network), and any of the relevant university rules. Also, such conduct as offending public order and morals or actions inappropriate under social conventions must not be carried out on the web.

Notes:

The following is an excerpt from the SINET regulations. For more details, go to the SINET page.
(http://www.sinet.ad.jp/)

Article 7: Member rules

The members must comply with the rules that follow:

1. Do not use the network other than for research and education, or administrative work in support of research and education.
2. Do not use it for the purpose of profit-making.
3. Do not interfere with the privacy of communication.
4. Do not disturb network operations.
5. Make utmost efforts to prevent inappropriate actions against the network or computer terminals with which you are connected.
6. Other rules that the director specifies separately.

3.1 Intellectual property such as copyright

Do not infringe on intellectual property rights that others possess. On releasing information on the web especially, one must pay utmost attention not to violate author's copyrights.

Notes:

All the works that other people have made are copyrighted. Therefore as a rule, content that was not made by oneself must not be included in the web page without permission. Also, one needs to note that even if one gets permission to duplicate certain content from the author, it does not mean the content can be publicly transmitted on the internet. Rights of public transmission (rights of making transmittable), in which the copyright holder gives permission for publication on the web, is a separate branch of rights from reproduction rights that permit normal duplication. Therefore one needs to have separate permission for transmission. Similarly, it should be noted that the "reproduction, etc., in schools and other educational institutions" provided in Article 35 of the Copyright Act merely refers to the act of "reproduction." All other actions that follow are not permitted. However, "quotation" without permission from the author is possible, if certain criteria within the copyright law are met.

Notes: (Term of protection of a copyrighted work)

The term of protection of a copyrighted work, as a rule, is 50 years after the author's death (if it is published under a corporate body, 50 years after the work is published). Therefore, if the work is from the Meiji period to pre-World
War II, it is important to see if the copyright is still protected. Also note that the term of copyrighted cinematographic works was changed to 70 years.

Notes: (Criteria for quotation of the copyrighted work)

Quotation, as an exceptional measure, can be made without the author's permission.

Article 32 of Copyright Act:

It shall be permissible to quote from and thereby exploit a work already made public, provided that such quotation is compatible with fair practice and to the extent justified by the purpose of the quotation, such as news reporting, critique or research.

From court cases, the following criteria have to be met for quotation:

- Legitimacy: There has to be a legitimate reason for the material to be quoted as it is. Without any contextual connection, it does not work as quotation.
- Clear division: There has to be clear difference between the author's text and the quoted author's text. In an academic paper, quotation is designated with quotation marks, but it can be done with underlines or different fonts or colors of the text on the internet.
- Clear indication of sources: The source of the quoted material should be as detailed as possible. For instance, page numbers should be added on top of the name of the periodicals or books. If it is quoted from other web pages, the URL should be mentioned as well.
- One's own material first, quoted material comes second: The quotation should come in place to supplement one's own work. If the amount of quoted material exceeds one's own work, it cannot be regarded as quotation.

Notes: (Moral rights of author (particularly the right to maintain integrity))

The author has the right to maintain the integrity of one's work. The Copyright Act does not allow distortion, mutilation or other modification that might be against the author's will, which is a moral right of personal nature that cannot be sold or transferred. It is therefore imperative to keep an author's work unchanged, when it is transmitted on the internet with permission or quoted with the proper criteria met.

Notes: (Non-copyrighted material)

No copyrights are applied to factual data such as economic indexes or meteorological statistics. However, when the factual data made by others is copied, put together and made into a new database (the so called non-creativity database), it must be noted that the creator of the database could call for criminal penalty or compensation for damage, as an illegal act under unfair competition prevention law or Civil Law

(Article 709). For this, the ruling on the database on car performance and other information "Tsubasa System versus System Japan" (Tokyo District Court, May 25, 2001) will serve as a reference.

For more information on copyright on the internet, refer to the following URL:

-Copyright Research and Information Center (CRIC): http://www.cric.or.jp/)

-National Institute of Multimedia Education (NIME): http://www.nime.ac.jp/)

3.2 Never infringe portrait rights and publicity rights

Notes:

It is considered that each person holds portrait rights as a human right. One should pay special attention on portrait rights when putting photographs on the internet. Photographs must not be put on the internet without the person's consent. In the case of prominent figures, it is considered that their portrait rights are limited as compared with the general public; however, they have what is called "publicity rights." These rights allow celebrities to receive profits from the use of their names and photographs. Therefore photographs of celebrities or athletes must not be published without permission.

3.3 Never transmit information that may cause trouble for others

One must not transmit information on the internet that could cause trouble for others. Such information includes that which is defamatory to others, and that could infringe on the privacy of others.

Notes:

Do not defame others either on one's own web page or on public message boards. It is possible that one could be sued for libel for such conduct, which could result in damage compensation under civil law, or a criminal penalty of up to 3 years imprisonment or imprisonment without work, or a fine of up to 500,000 yen. Attention is required when dealing with other people's private information. Privacy in general refers to the so-called sensitive information an individual does not want others to know about. However, there is no clear-cut definition in law and court cases, and therefore it is not very easy to deal with. Thus, when dealing with others' information, if there is a possibility that the transmission on the internet might affect the others, one should not put the information on the internet. (If there is a slight chance that the transmission could affect the other person, the information should be withheld. Even when one assumes that it would bring about positive results, it could produce a non-desirable result for the other person.)

3.4 Risks of releasing information on finished or un-finished research results

Always be cautious when deciding whether or not it is appropriate to put information on finished or un-finished results of studies on the internet.

Notes:

When the project is the result of collaboration with a private business or other researchers, always pay close attention so as not to violate the nondisclosure agreement. If there is a possibility of a patent application, publicizing the findings of studies on the internet could result in disqualification due to "lack of novelty," which is a condition for the patent application.

3.5 Corporate names and logos

Always consult with the other party when putting corporate logos on the internet on occasions of academic conferences and symposia.

3.6 Risks of releasing portraits on the internet

Think about the risks of putting your own photograph on the internet.

Notes:

It is important to weigh the pros and cons of releasing one's own name or photograph on the internet. Caution is needed because in some cases, one could be accused of or defamed for no reason, or be tripped up in one's wording or remarks, or worse, become a stalking victim. It is advised that one should be even more cautious when putting information or group photographs of the laboratory members on the internet.

3.7 Never transmit information in violation of laws and regulations or public order and morality

Do not transmit information that is in violation of laws and regulations, not to mention harmful information and the kind of information that is against public order and morality.

Notes:

Other than obscene documents and graphics, harmful information includes the following:

- information that could attract illegal actions (firearms or explosives, banned drugs or narcotics)
- information that could solicit suicide
- solicitation for pyramid schemes
- information that contains harassing descriptions

For detailed description of harmful and illegal information, refer to the operation guidelines on the web site of Internet Hotline Center (http://www.internethotline.jp/).

4. Digital Archives

It is imperative to go through the necessary procedures before releasing classical material on the internet.

Notes:

In general, copyrights are expired on classical material (copyrighted material is protected up to 50 years after the author's death). However, there are many other agreements that are made other than copyright. Some examples include ownership rights, or agreements that were made at the time of digital archiving bearing the cost of archiving, etc. Therefore, careful assessments are needed when releasing digitalized information on classical material. For example, some classical material that the university possesses could be items or a collection of items a local family requested the university take care of. Or in some cases, agreements were made for the university to digitally duplicate the artifact on condition of not releasing it on the internet. Court rulings have found that "when releasing duplication of any contents that are in the public domain, if acquired by legitimate means, it is not necessary to ask for permission of the original owner". However, in practice, there are cases in which monetary compensation could be assessed. It is more desirable to have a detailed preliminary discussion with the donor of the material (digital archive cooperator), because in some cases, the way that the digital information is released on the internet becomes the focus of trouble. It is also strongly advised that written consent should be exchanged between the two parties in order to avoid subsequent troubles and regrets.

*Yan Zhenqing Jisho kenchu shinkoku shinchou case
(Supreme Court, January 20, 1984)

Yan Zhenqing was a leading Chinese calligrapher in the Tang Dynasty. A publisher owned the photographic plates that duplicated Yan's work "Jisho kenchu shinkoku shinchou" and put them together in a book for publication. The owner of the original work of Yan sued for suspension and disposition of the books.

The publisher acquired the photographic plates in a legitimate way; it was not a case of stolen property or illegal photographing. The Supreme Court ruled that the property rights on the original artwork only apply to the right to exclusively owning the tangible entity, but not to the duplicated photographs. The Court also ruled that: "At museums and art galleries, it is allowed to charge a fee for shows or authorizing permission to take photographs because of the proprietary privileges for the original work. It appears as though the owner exclusively possesses the rights to give permission to duplicate the original work, but it merely reflects the effect that the owner has the original work as a tangible entity, which belongs to the public domain." There are detailed notes on the FAQ page on the web site of the aforementioned Copyright Research and Information Center (CRIC):
http://www.cric.or.jp/qa/sodan/sodan7_qa.html

5. Policy on Links

Exercise caution when providing links on web pages.

5.1 It is recognized that providing links is customarily done without obtaining permission. However, putting links on other hierarchical pages is not always regarded the same as the top page. Therefore, try providing links on the top page.

Notes:

There are overseas cases where the validity of a deep link was the focal point in lawsuits. The courts have ruled negatively in cases of providing links so as to disable banner advertising, or showing others' content such as news stories from other web sites as one's own.

6. Adherence to rules and regulations; prohibition on use for purposes other than the original intent

6.1 Prohibition on the use for purposes other than the original intent

Those who release web pages must comply with these guidelines as well as related rules and regulations on the use of university information systems. One must not use the web page for purposes other than what are outlined in the university regulations and SINET regulations. The university information system facilities and SINET are provided for education and research promotion, as well as carrying out job duty and support services. Therefore for those who transmit information, there must be a line between private and public matters and intention not to release information that is irrelevant to the purposes of the system. A typical violation of this rule is the case in which one uses the university facilities not for research purposes but to gain profit for commercial purposes.

Notes:

The following are examples of use deviating from the original purpose, and students are advised against them:

- advertising on web pages about private tutoring
- making a profitable website with affiliate advertising

Faculty members should also take care in introducing their own books. Too much information on advertising and the sale of one's books other than a mere introduction or book sales as students' textbooks can be regarded as excessive or a violation of academic network use policy.

6.2 University regulations prohibit the following activities:

(a) Commercial activities
(b) Activities concerning specific political parties or religious groups
(c) Damaging the reputation of and demeaning the University of Tsukuba
(d) Campaign activities as described in Public Office Election Law
(e) All other violations of university regulations

7. System Security policies

7.1 When building web pages, be aware of security.

Operating systems and application software should always be updated with the latest patches. The same applies when the home page building is outsourced to external contractors.

Notes:

The server system, needless to say, must be kept secure as much as possible. When web contents are out-sourced, the security technology should be an important element in the contract with external contractors, not to mention design and accessibility. Also, an appropriate amount must be invested for security. The university is also held accountable even in the case of external contractor involvement.

7.2 Hidden directories

Never embed information on the web page that one does not want to be released to the public, even in the form of a hidden directory.

Notes:

The so-called "hidden files" and "hidden directories" that are not linked directly from the web page can be picked up by robot-type search engines. Therefore, never put information that must not be seen by the general public under public_html, which is an often-used procedure to provide information to selected members. If necessary, do so only for a limited period of time, or use other means such as basic access authentication.

An incident occurred in the past when an instructor tried to release the grades only for auditing students and left the information under a hidden directory on the server, which was later revealed by the search engine and released to the general public. In any event, never put information on the web server that must not be seen by the general public as stated above. Also, never use dates and file names for a URL that could easily be assumed by others. Even if a link is not visible from the top page, people can guess the URL and obtain access to sensitive information. There was a case in which the results of a university entrance examination were leaked before the announcement day because of a URL that was easily guessed.

7.3 Server capacity and network resources

Try to secure enough capacity for the server and network before setting a server for a web page opening, so it can deal with the access volume.

Notes:

It is often the case that the laboratory server is used as part of the preparation for academic conferences and symposia.

However this tends to overload the system.

When large volumes of documents are exchanged, special consideration has to be made for one's own server as well as the capacity of the system upstream. This applies with the university and department servers, when the announcement is to be made for the results of the university entrance examination.

8. Scope of liability on the administrator of web servers and message boards

It must be noted that the server administrators are liable inside and outside of the campus. Internet Service Provider Law (ISP Law) in particular, regards administrators of websites and message boards as the providers of the "specified telecommunication service." Therefore, such administrators are cautioned to be aware of what is regulated in the ISP Law.

Notes:

ISP Law regulates limitation of liability for damages for specified telecommunication service providers and the right to demand disclosure of identification information of the senders.

The administrators of websites and message boards are regarded as "specified telecommunication service providers" in this law.

When there is an infringement of rights (infringement of human rights or intellectual property rights) by others on the web, the administrator of the web is required to eliminate the infringing content. If the elimination does not take place immediately, the administrator is liable for the damage done for the victim of the infringement. However, if the administrator eliminated the information according to the procedure in the ISP Law, the administrator is freed from liability for damage. Also, if it is done according to the guidelines of ISP Guidelines Association, it is expected that the court would deny responsibility of damage liability for the administrator. For further details, please refer to the following URL:
http://www.telesa.or.jp/consortium/provider/index.htm

When there is a demand for disclosure of identification information of the sender because of an infringement of rights taking place on one's webpage, but the infringement is not very clear, the administrator is not obligated to disclose the information immediately. The same applies to an inquiry from an investigating authority; unless there is a warrant, there is no obligation to cooperate with the investigation by disclosing the information.

9. Inquiry for the above guidelines

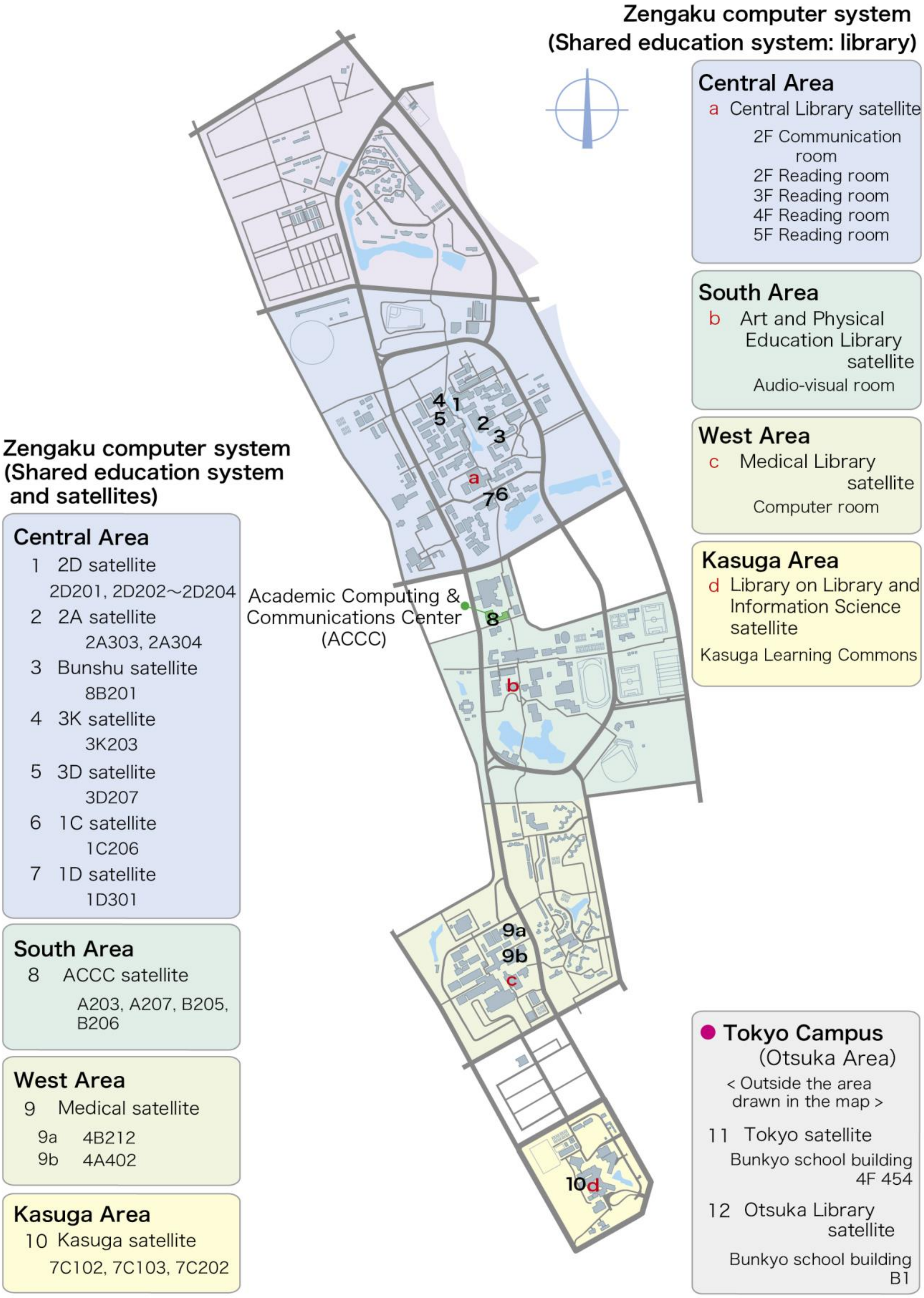
In cases where the interpretation of the above regulations is not clear or are beyond the scope of these regulations, the web administrators must contact, report to and follow the instructions of the department technical personnel (Chairperson of the Sub Network Administration Committee) when it is urgent and an immediate response is required.

Note:

These documents have been translated from original Japanese documents. If there are any differences between the Japanese document and the English document, the Japanese version shall take precedence.

User's Guide to Zengaku and Other Computing Systems at the University of Tsukuba
Eleventh Edition (April 1, 2017)
Academic Computing and Communications Center, University of Tsukuba

Satellites of the Zengaku Computer System



Zengaku computer system (Shared education system and satellites)

Central Area

1 2D satellite
2D201, 2D202～2D204

2 2A satellite
2A303, 2A304

3 Bunshu satellite
8B201

4 3K satellite
3K203

5 3D satellite
3D207

6 1C satellite
1C206

7 1D satellite
1D301

South Area

8 ACCC satellite
A203, A207, B205, B206

West Area

9 Medical satellite

9a	4B212
9b	4A402

Kasuga Area

10 Kasuga satellite
7C102, 7C103, 7C202

Zengaku computer system (Shared education system: library)

Central Area

a Central Library satellite
2F Communication room
2F Reading room
3F Reading room
4F Reading room
5F Reading room

South Area

b Art and Physical Education Library satellite
Audio-visual room

West Area

c Medical Library satellite
Computer room

Kasuga Area

d Library on Library and Information Science satellite
Kasuga Learning Commons

● Tokyo Campus (Otsuka Area)
< Outside the area drawn in the map >

11 Tokyo satellite
Bunkyo school building 4F 454

12 Otsuka Library satellite
Bunkyo school building B1