GUIDELINES FOR INFORMATION ETHICS AND SECURITY

Tokyo Institute of Technology

東京工業大学

Contents

Information Ethics Policy of Tokyo Institute of Technology

(Objective)

This policy aims to prevent any act which is considered to be unethical, based on legally and/or socially accepted ideas regarding the use and disclosure of information at Tokyo Tech. It also aims to promote appropriate use of information, ensuring academic freedom, freedom of thought and expression, thereby enhancing education and research.

(Observance)

Those who intend to use or transmit information at Tokyo Tech shall recognize that the information is of value and vastly influential, and thus shall be responsible for proper use of this information. Any actions with regards to the use and transmission of information shall observe the items listed below.

(1) Respect the owners rights when utilizing legally protected information involved in copyrights, patent rights, and other intellectual property rights.
(2) Respect the secrecy of confidential information and data.
(3) Respect the privacy of others and avoid abusing others' rights, when manipulating information of a personal nature.
(4) Neither collect nor transmit information that is considered to be socially and/or morally unacceptable or possibly offend others.
(5) Administrators with access to information and communication must not use this information for personal use or any other use which is not required to perform their duties.
(6) Do not apply information supplied for a certain purpose to any other purpose without prior approval of the suppliers.
(7) Cooperate to realize smooth system operation for processing, accumulating information and communication.
(8) Use systems for processing, accumulating, and communicating information and data only for education and research purposes.
(9) When handling and/or transmitting information, keep in mind the effect of this information on both the public and social development.

Introduction

Information gains important significance only when it circulates in society. Its handling comes with a variety of restrictions that have been imposed to ensure smooth development of society. In particular, information flowing through networks connected to computers may possibly expand its influences to a global scale since its transmission is both fast and in multiple modes. Taking this into consideration, we should pay careful attention to its handling. The following pages give Tokyo Tech students and employees a summarized description, in a plain expression, of the rules and principles of information handling (information morals) that should be observed in the modern society. The contents are roughly classified into two folds; ethical and legal regulations, and countermeasures against system security problems. To make full use of both information and information systems and enjoy a fruitful life, be sure to pay attention to the items that should be observed so that we should not make mistakes. Also, bear a defensive manner in mind so that we might not get involved in an unexpected trouble.

Ethical and Legal Regulations

1. Copyright

The Copyright Law protects authors’ rights to information contained in an electronic medium, such as the Internet and CDs, as well as that in printed matter. Take full care not to violate it.

For the cases outlined in the box below, you may duplicate and use such information without permission, however, always be careful so that copyright owner's profit may not be unduly impaired.

You should not duplicate electronic information by breaking copy protection or other technological protection.

- Duplication for private use
- Duplication under specific regulations (e.g. duplication at a library)
- Citation by clearly giving a source of original work in its main portion
- Duplication for educational purposes in a scope that will not hinder the sales of an original work or duplication for use in examination questions
- Duplication of programs for backup
- Performance for non-profit purposes (however, drama performance at a cultural festival at schools is now exposed to a possible revision of a law)
- Utilization for report of current affairs, etc.

You should also exercise care in using edited work and work accumulated as a database other than the original, since secondary copyright may be generated in them. Also be careful that, almost all the electronic publications prohibit bulk downloading of many files by means of an automatic downloading program.

In addition to the authors' rights, neighboring rights are provided to performers, record manufacturers, and broadcasters. Hence, you should not infringe these rights. Wire/wireless broadcasters are considered to be included in the category of broadcasters, but persons offering information through the Internet are not included in this category.

However, be careful that this fact does not signify that any persons may duplicate or resell information available through the Internet. When disclosing other party's work through the Internet, you should acquire its permission so that you may not infringe its rights to make the work transmittable (or to upload its data to a server in the Internet).

In addition to duplicating rights, stage rights, and other property rights, moreover, personal rights are protected for an author to maintain identity of his/her work, to indicate or disclose his/her name in relation to his/her work when it is made public. Hence, it is not permitted to publish a work whose contents are revised without an original author's approval as if it were the work of the author.

2. Software license

Software is generally sold in a form of permission to use it. The permission provisions usually prohibit the installation of the software in more than one computer unless a site license is acquired. If you are requested to take a similar action, definitely refuse it. Even if your supervisor or boss asked to do so, you should show a resolute attitude towards him/her.

3. Precautions on the use of e-mail, bulletin boards, and websites

In the process of information exchange on the Internet, we sometimes commit criminal and/or illegal acts unknowingly. Acts of gambling, pyramid sales, or fraud are crime with criminal penalty regardless of an amount of money. Watch out not to take part in such illegal acts through a terminal or cellular phone by believing clever salesmanship. Otherwise you could become an offender. In recent years, the number of fraud cases through electronic mail in which false loan payment is demanded or charges for use of adult sites are invoiced has been increasing. Once you are damaged, your losses are unlikely to be repaid. So, take care of not being a victim of a fraud. Since disclosing your mail address to the public will increase the opportunities for you to encounter a fraud, take this fact into account when doing so. Be careful of disclosing it to the public because there have been such cases as your address is registered to a spam mail receiver list and you are compelled to disposing of an enormous amount of mails you do not want to receive.

Keeping yourself unaware of privacy and human right issues may sometimes put you in a serious plight. You may have access, for example, to mailing history while engaging in server administration, but transmission between other parties is a matter of privacy. If you are in a position to access such logs, pay thorough attention in handling them. Needless to say, never read other persons' mails secretly.

Avoid doing something unwanted by others, such as sexual harassment. What interests you might disgust the others. Always endeavor to exchange information taking into consideration the feelings of others. Communications by mail tend to be different to usual conversation. Always stay emotionally controlled.

Concerning legal issues, do not justify your actions by yourself, though a matter against public order and customs or of defamation has to be put to judicial judgment. Even if other persons are not blamed for their illegal or unlawful acts, it is never acceptable that you can take similar action. Refrain from any actions that may arouse other persons' suspicion. Avoid placing yourself in a compromising situation.

4. Information disclosure and protection of personal data

The Internet has made it possible to globally disclose and transmit information through websites and/or e-mail. This is indeed wonderful and you may naturally want to transmit a variety of information. But, as previously mentioned regarding e-mail, be fully aware of the fact that disclosure in the Internet involves danger. It is dangerous to disclose data that, taken as a whole, help identify a particular individual. If a full set of data, for example, name, address, telephone number, and birthday are known, other persons with malicious intent may identify themselves as you. (This is known as "identity theft".) When handling another's data, it requires more care than in handling your own. Be careful not to disclose other persons' information without their prior approval. The Personal Data Protection Law provides for a variety of regulations on handling personal information for protecting personal rights of individuals.

5. Observance of other laws

Observe the provisions and tenors of laws and refrain from doing the following acts:

- To secretly find other person's account and passwords and make access to protected information by taking advantage of browser security holes hidden in a program
- To break into computers under other persons' custody through terminals connected to them or through the Internet and obtain, erase, and/or modify information stored therein
- To transmit meaningless electronic mails (spam mails) that cause other persons to feel unpleasant or to forward the spam mails you have received to others
- To make services available on the Internet malfunction by sending a large amount of requests to them
- To use trade names of enterprises and/or commodities on your websites without prior approval
- To illegally obtain trade secret, such as enterprise's client lists
- To put personal information to use other than the purpose which you promised when collecting it
- To disclose on the Internet or notify a third party of the results of joint research that should be kept secret

6. Working rule (applicable only to employees)

The working rule of Tokyo Institute of Technology includes duties for its employees. They have obligations to do the same as they were national government employee as listed below:

- Obligation to devote oneself to duty
- Obligation to obey laws and regulations, the Institute’s rules, and supervisors’ instruction
- Obligation to keep secrets and confidential information learned on work
- Prohibition of actions to defame the Institute or dishonor it
- Prohibition of actions to disturb the Institute’s discipline and order

In terms of information ethics, for example, using a personal computer for private processing during working hours, transmitting files containing the Institute’s secrets to others outside campus, and writing items not directly related to office work on electronic bulletin boards will violate the working rule. If you violate such obligations, you may be subject to disciplinary punishments such as disciplinary dismissal, suspension from office, salary reduction, and official admonition, or reprimand, strong warning, and warning.

7. When trouble occurs

Notify the Information Ethics Committee, when trouble occurs.

Mail address: cce@cs.titech.ac.jp

Computer Security

In addition to observance of ethical and legal matters, from the security point of view you should ensure to protect your data in your PC as well as other's data, when your PC is attacked by virus etc. or hardware troubles occur.
The following describes the minimum requirements concerning computer securities and adequate attention should be paid while operating computers.

1. Backup

Each user's data are precious assets to them. Bear it in mind to back up your data regularly for yourself. Periodic backup promises constant conservation of your precious data even in the case of reinstallation of the OS. However, backup media have their own service life and the technical environment to read them may be changed as a result of rapid progress of technology. Taking into account these situations, you should take the most appropriate strategic countermeasures for short- and long-period backup operations. It is one of the smart alternatives to make use of external archives for storing non-secret data.

2. Countermeasures against virus

It is quite well known that a large number of viruses caused significant damage in recent years. To underestimate them is very dangerous since some of them destroy data. Your computers may become infected with viruses without your knowing, and then through networks viruses may destroy others' data in some cases. Pay attention to the following.

(1) Endeavor to install virus-checking software in your PC.
Make it a rule to periodically update pattern files in addition to the installation of such software. Close attention and daily inspection will protect you from damage even in an unexpected attack from viruses.

(2) Be careful that virus-checking software is not completely secure even if pattern files are regularly updated, a danger from infection can occur immediately after a new kind of virus is created. Hence,

- Do not open a mail from an unknown sender.
- Endeavor not to open those files which are attached to a mail from a known person if its contents are unnatural.

(3) Some viruses are infected merely by browsing a website. Refrain from visiting doubtful websites for entertainment.

(4) Refrain from installing unreliable free software, because by installing such programs, there is a danger of being buried unwanted program which is so-called spyware program at the same time.
A spyware program will silently report important personal information and PC operation history to external sources.

3. Security update

Never fail to run security updating of the OS and application software installed on your PC. While it's tempting to avoid the hassle of updating your software, you may find yourself in an extremely risky position without knowing it. Make it a routine to confirm whether or not security updating is needed when starting your PC.

4. Password administration

A password is like a key for utilizing an information system. If your password is leaked, unauthorized third parties may utilize the information system without permission. It is as if your house is robbed because your key has been stolen. Pay attention to the following points regarding password administration.

(1) Do not show your password to other person, even if he/she is your friend. Avoid writing down your password on paper.

(2) Avoid using a simple password. Use password long and complicated enough to prevent other people to guess it.

(3) Refrain from using the same password over a long period and make it a rule to change it occasionally.

(4) Phishing is prevailing. In the phishing fraud, a person disguises as if he/she were an authentic administrator, prepares a false website looking like a true one, persuades a user to log in his/her password, for example, by insisting a test after system update, and uses the password illegally. Be fully careful that you should not be deceived by such a mail, because no system administrators make such a request at all.

5. File sharing setup and network administration

Pay thorough attention to file sharing setup so that no unnecessary files are shared. You should confirm how a newly created file or folder is included in the sharing setup. Firewall can be set up by a router as well as an individual PC. Make it a rule to keep ports for external access closed unless used.

6. Actions to be taken against system trouble

It is out of the question to perform a destructive act on an information system or assets. Also, be careful of the effect of unintended actions including misoperation or a seemingly harmless action made for just curiosity since they may sometimes harm on information system or other persons' information assets. Should such an event occur, never attempt to conceal it, but immediately notify a system administrator of this fact so that damage may not become more serious.

Q&A

Q1: (Connection of a private computer of private property with the Institute’s network)

May I connect my personal computer to the Institute’s network? If permitted, what points should I pay attention to?

A1: Follow the instructions given by a network administrator of a group you belong to (e.g., laboratory, department. etc.) . Since public space such as campus cafeteria is provided with wireless LAN facilities, students may connect their own PC with the network. Before connecting your PC, be sure to confirm that it is free from viruses.

The Institute has suffered from virus damage, and some of these came from students’ personal computers. Be careful of sharing setup and firewall settings.

Q2: (Installation of software as the Institute’s asset to a private computer)

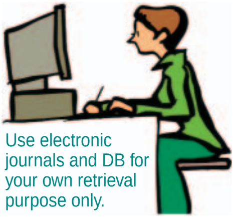
May I install software purchased by the laboratory to my own personal computer?

A2: This is an issue that should be considered from the viewpoints of a software license agreement and the application of the Institute’s assets. So long as you observe the license agreement concerned, there will be no problems. Since the software has been purchased by the laboratory, it should be applied to the objectives related to the laboratory activity, like the case with other items. Actuallly, however, it is rather difficult to clearly discriminate them. In other words, be careful of the fact that you cannot indicate that you have not applied it to your own private objectives, because it can be applied so.

Q3: (Document retrieval)

A friend of another university asked me to retrieve documents by means of database and electronic journals available in the Institute. May I do that?

A3: The Institute utilizes the database and the electronic journals under license agreements and restricts the scope of users to faculty members, students, staff, and others belonging to it. Their use of database for personal purposes other than research and educational purposes and/or offering retrieved results to other persons violate the agreement. If such actions are discovered, the database provider will suspend access for the whole Institute. Hence, be sure not to do such actions.


Use electronic journals and DB for your own retrieval purpose only.

Q4: (Database downloading)

To what points should we pay attention when downloading data and documents from the database and scientific magazine sites?

A4: In the past there were many cases in which Tokyo Tech faculty members and students downloaded a large volume of documents and the database provider suspended access for the whole Institute. Since mechanical downloading by means of software violates the agreement, it is not permitted to download documents that coincide with specified key words by using scripts in a single procedure. Even in the case of manual operation, repetitive downloading operations for more than one hour is sometimes regarded as mechanical. Downloading of a large volume of data for educational or research purposes needs the provider's approval. If you need to download a large volume of data, contact the Institute Library staff.

Q5: (Copying of update software)

In the past, the whole network of a department was affected by a virus when a personal computer infected with it was connected to the network. In the case of Windows, for example, a regulation was proposed that the network should not accept a computer not yet utilizing the Windows security update service or having no updated virus definitions. But it would be inconvenient if a visitor cannot connect his/her PC to the network. Moreover, if a PC cannot be connected to the network, its owner cannot utilize the Windows update or update virus definitions. It is concluded as a result that we should prepare a CD that will secure the safety of the network within the department. Can we carry out this proposal?

A5: In principle it is not permitted to copy and distribute a software program for other person's use even if it is free. The reason for us to prohibit copying of a software program and putting it to other person's use is to protect property rights from being infringed by its use without permission. On the other hand, the Windows update is a free service available to Windows users for enhancing the product reliability and it will never be blamed if help is offered for its better utilization. However, it is advisable to refrain from copying a virus definition file because it contains programs applicable to other products.

Q6: (Disclosure of own paper)

May I disclose my paper presented at an academic conference or meeting in my own website?

A6: It is general practice for a researcher to utilize his/her website for disclosing his/her paper presented at the academic meeting or contributed to an international conference or an academic journal at the time of presentation or contribution. However, some academic societies have severe regulations. So, consult with a corresponding society and obey its regulations once your paper has been accepted.

Q7: (Disclosure of research progress)

May I disclose the progresses of my own research on the Internet?

A7: Even if you consider the research you are involved in as your own, it is quite reasonable that your research is carried out under your supervisor's guidance or suggestions or assisted by colleagues' ideas or unpublished research results. Your disclosure of the progresses of your research contents on the Internet may sometimes result in unexpected disclosure of your supervisor or colleagues' ideas. It is also probable that an unknown person may read your ideas on the Internet and publish them in his/her own paper earlier than you do. In such a case, it is rather difficult for you to show that his/her paper is based on your research results. This means that you should be more cautious in disclosing the progresses of your own research contents on the Internet and other publication media. If you are a student, it is recommendable to consult with your supervisor.

Q8: (Utilization of computers and networks or prohibition of their use for objectives other than designated ones)

Issues of corporation of universities are recently discussed on networks and such mailing lists are reported. I have been reading them and have raised some points as to the issue of the university corporation through the networks. Are these actions punished?

A8: Such actions do not directly meet research and education purposes but are one of the important actions for academic people to consider the future of a university. On the other hand, computers and networks form an integral part of general information infrastructures and support the university operations. Although your actions seem harmless in this respect, the point at issue is whether or not those actions deserve those done by an academic within his/her office hours, and they will be judged from this point of view.

Q9: (Is telling the truth slander?)

I have once notified all the members in a mailing list of a fact which a friend of mine did not want to be made known. I did not mean to slander him/her and thought that I had simply told the truth. However, he/she does not seem to permit it.

A9: It is understood that spreading a false rumor is immoral, but telling the truth is actually considered slander in some cases. Actual slander often seems to occur unknowingly in such a case. Always be careful when disclosing information because it sometimes leads to a case of the defamation of character.

Q10: (What is the scope of communications between individuals?)

A friend of mine once returned a mail, rather strongly revoking mine. If he/she gave that reply only to me, I would have treated it as give-and-take of individual opinions. Hence, is it permitted to distribute his/her reply to the members in a mailing list in a form of CC without their approval?

A10: It is probable in a sense that this is a case of strong criticism in public. Such a case may sometimes result in a case of the defamation of character. Be sure to acquire a receiver's approval before referring to or attaching his/her mail.

Copy protection, publication of paper, utilization for non-intended purposes

Q11: (Copy protection)

If I use a software program to nullify copy-controlling functions of a CD and a DVD and duplicate its contents, does it infringe the copyright?

A11: Article 30 item 1 of the Copyright Law admits that a user may duplicate a work if the user intends to use a duplicated one within a limited scope of personal use or use in a family or equivalent ("duplication for private use"). However, it specifies that duplication of a work while recognizing that it can be duplicated because technological protection means have been avoided does not fall within the said duplication for private use (Article 30 item 1-2).

In the case of the question above, it is not considered as duplication for private use and infringes the copyright (duplicating rights) because you use and duplicate a software program by which you can nullify the copy controlling functions.

Q12: (Utilization of a program among more than one user by means of a client/server system)

I want to allow a client to take a program out of the Tokyo Tech client/server system and temporarily use it after I store it in a server. What kind of legal care should I take in this concern?

A12: You should receive a permission from a copyright owner of the program copied in the server as to the right to enable it transmittable in addition to the duplicating right of that program. However, there remains a problem as to whether or not the "public" of the public communications be applied if the number of client's computers is small. If the client uses it permanently rather than temporarily by downloading it from the server, site license is necessary.

Q13: (Utilization of an electronic dictionary and the like stored on the server by more than one person)

I want to use a non-program work such as an electronic encyclopedia on the server in the Tokyo Tech intranet system and put it to use among many clients. What precautions should I take in such a case?

A13: It suffices if you receive a permission of copying right for one copy of the electronic encyclopedia duplicated on the server. Assuming that each page of that encyclopedia displayed on each client's screen is a duplication under the Copyright Law, each client would infringe the copying right in his/her side. If he/she does not keep it permanently, it will not be regarded as infringement. However, the matter is not so clear if the issue of cache is involved.

Q14: (Illegal access to and destruction of computer programs)

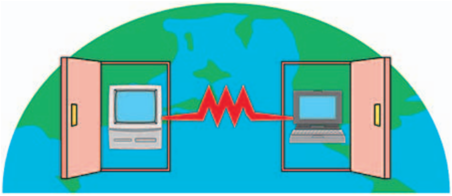
What kind of illegal access to and destruction of computer programs should we be careful about?

A14: Typical attacking patterns include those of a “virus,” “worm,” and “Trojan horse.” A virus is a program that parasitizes and infects others and proliferates while hiding in the operation of a host program after copying itself as a part of other programs. Unlike the virus, a worm is a program that proliferates by itself. These two are programs that enter into a computer regardless of the computer owner's desire. On the other hand, a Trojan horse causes a program user to suffer from illegal acts that have been inserted in that program by its developer once the user installs it. In recent years, however, illegal accesses and their routes are more and more skillful to a degree that may make the above-mentioned classification meaningless.

Q15: (Countermeasures against illegal computer access)

What is the point of which we should be careful in preventing illegal computer access?

A15: Windows and other complicated, large-scale OS contain security holes (that may be regarded as defects in the software) and crackers make access to it by finding them out. Since their manufacturers have publicized a “program for correcting the program” involving security holes already found, endeavor to correct them by yourselves by using such a program. This operation is usually called “patching.” It is also significant to connect your computers with a site for which a dependable firewall has been provided and at the same time to introduce a firewall into your own computer. It is further important to use a virus-checking program to be on constant alert for viruses.



Take full measures against viruses.

Be sure to introduce a firewall and
a virus-checking program.

Information related to Tokyo Tech website

- **Tokyo Institute of Technology Information Security Policy (in PDF form)**
  http://www.jyohosyorika.jim.titech.ac.jp/security/policy.pdf

- **Declaration of damage by computer viruses and illegal access**

  Virus declaration form
  http://www.jyohosyorika.jim.titech.ac.jp/security/virus.htm

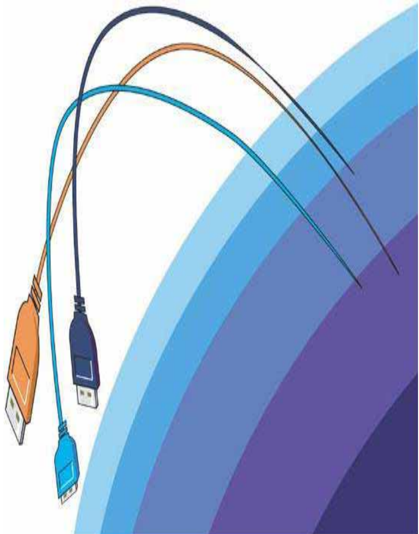
  Illegal access declaration form
  http://www.jyohosyorika.jim.titech.ac.jp/security/crack.htm

Since we report the cases of computer viruses and illegal accesses to E-Education Promotion Room of the Ministry of Education, Culture, Sports, Science and Technology, any victims should report their damage in a declaration form to:
Scientific Information Department, Information System Planning and Editing:
jyoho.gyom@jim.titech.ac.jp

- **Tokyo Institute of Technology, Information Ethics Committee**
  http://www.titech.ac.jp/rinri/

Information Ethics Working Group

YONEZAKI, Naoki	The Committee Chairperson; Prof., Graduate School of Information Science and Engineering
SAKAI, Yoshinori	Vice-chairperson; Director, Global Scientific Information and Computing Center, Prof., Graduate School of Science and Engineering
ISHIKAWA, Ken	Assoc. Prof., Graduate School of Science and Engineering
WATANABE, Osamu	Prof., Graduate School of Information Science and Engineering
WAKITA, Ken	Assoc. Prof., Graduate School of Information Science and Engineering
KIMURA, Koji	Prof., Graduate School of Information Science and Engineering
KANEKO, Hironao	Assoc. Prof., Graduate School of Decision Science and Engineering
ITOH, Toshiya	Prof., Global Scientific Information and Computing Center
YOKOTA, Haruo	Prof., Global Scientific Information and Computing Center
KOJIMA, Satoshi	Assoc. Prof., International Student Center
SAKURAI, Minoru	Prof., Center for Biological Resources and Informatics
HENMI, Tatsuyoshi	Head, General Affairs Division, General Affairs Department
TANAHASHI, Akira	Head, Library Division, Academic Information Department
MIURA, Masakatsu	Head, Information Infrastructure Division, Academic Information Department
FUSE, Isamu	Head, Information System Planning Division, Academic Information Department
YOSHIDA, Yoshikazu	Chief, General Administration Section, Student Affairs Division



GUIDELINES FOR INFORMATION ETHICS AND SECURITY

Publised in April 2005
Tokyo Institute of Technology