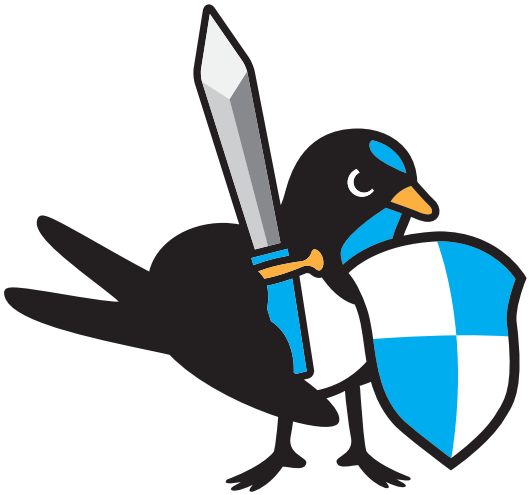
Guidelines
for Information Ethics and Security

《 2nd Edition 》



Tokyo Institute of Technology

A Quick Guide to Information Ethics and Security

This page provides readers with the basics of information ethics and security. For further details, please refer to the relevant sections, including the Q & A, of this handbook.

【 Ethical and Legal Regulations 】

Use of emails and the Internet	Be careful not to commit or get involved in Internet fraud. Check the legitimacy of the source of information you receive. Do not use information technology to harass others.
Use of SNS and blogs	Be aware that anyone can browse your social networking sites.
Protection of personal data, privacy, and human rights	Protect personal data and privacy of others as well as your own.
Researcher ethics	Students, as researchers, must hold high ethical standards.
Protection of information and intellectual property	Be careful not to infringe copyright.
Use of software	Licenses must be acquired to use software.
Compliance with the law	Failure to comply with existing laws may result in punitive measures.
Tokyo Tech regulations	Faculty and staff are obliged to follow Tokyo Tech employment regulations.

【Information Security】

Mobile devices	Be careful not to lose mobile devices. Take precautions against information leakage.
Data backup and security updates	Regularly back up the data and install security updates on your computers.
Password management and hacking countermeasures	Always use strong passwords.
File sharing and network management	Implement access control.
How to deal with system failures, unauthorized access, and data leakage	Contact the relevant system administrator and Tokyo Tech CERT immediately.

Guidelines
for Information Ethics and Security

Information gains considerable weight when it is allowed to spread through society. In today's world, vast amounts of information are transmitted at high speeds over the Internet, making it possible for such information to impact the whole world in an instant. In order to allow our society to adapt to and advance in this information-intensive age, various restrictions have been devised regarding the ways to handle information.

This handbook has been written to provide students, faculty, and staff of the Institute with a concise guide to regulations and ethical principles that should be observed when handling various kinds of information. Institute members are expected to understand and follow these guidelines so that they may benefit from utilizing information and the Internet safely, responsibly, and wisely.

The handbook is divided into three parts. The first part is concerned with ethical and legal regulations, the second with information security, and the third is a Q&A part with specific cases and relevant advice. A list of relevant links is also provided in the appendix.

In the table of contents on the following page, section titles have been tagged with the letters U, N, P, S, and W. These tags indicate how each section is related to the following items that comprise the information infrastructure:

Contents

Guidelines for Information Ethics and Security

Ethical and Legal Regulations

Although the rise of the Internet has made new and diverse ways of exchanging information possible, it has brought illicit conduct closer to the lives of its users as well. In order to truly benefit from this technology, it is important for users to understand that with greater freedom comes greater ethical and legal responsibilities.

Use of Emails and the Internet

The ease of communication over the Internet means that there are now greater chances of people getting engaged in unlawful activities without taking time to consider the seriousness of their actions. For instance, smartphones have made access to gambling, pyramid sales, fraud, and the trade of illegal drugs as easy as a few taps. These acts, however, are criminal offenses that incur punitive measures, and you must not allow your curiosity or solicitation by others lead you to take part in such conduct.

Email fraud involving false claims for debt repayment and charges for adult sites are also rampant. Once you make the payment, it is highly unlikely for you to ever get your money back. It should be noted that the risk of being targeted by fraud will rise by making your email address public. Time will be lost sifting through spam that inundate your account.

Internet users may also encounter online fraud simply by browsing websites. Users who do not check URLs properly are sometimes deceived into thinking that a fake site they have accessed is the legitimate site they are looking for. These are called phishing sites and are designed to steal people's valuable information such as user names and passwords. Always check the URLs of the websites you access. If there are telltale signs of fraud, such as the sites not being SSL certified (i.e., the URLs do not start with https), do not enter any information.

Email harassment is another problem that has arisen in recent times. Avoid sending emails that may be perceived as sexual harassment. Conduct you may find acceptable may be offensive to others. Be considerate.

Furthermore, keep in mind that, unlike face-to-face communication, emotions can quickly reach boiling point when emails are used. Use self-restraint and never send a message

when you are angry. Reconsider your response once you have calmed down.

Finally, it should be noted that cults and terrorist organizations also use the Internet to recruit new members.

Use of SNSs and Blogs

There are currently many forms of social media available, from microblogs, such as Twitter, LINE, and Google+, to social networking sites (SNSs), such as GREE, Mobage, and Facebook.* These media are essential tools for facilitating self-actualization, and what are posted on these sites are protected under the freedom of expression. Although the Institute currently imposes no restrictions on personal usage of social media, you are expected to exercise discretion when posting information.

For instance, through posting accounts of your everyday life, you may inadvertently end up disclosing too much personal information. Also, your posts may unexpectedly trigger adverse responses from those who read them, which may lead to your site becoming a target of abuse.

Make sure you understand the implications of disclosing information on social media in order to ensure safe use. When creating an SNS account, always check its setting. SNSs often make their account holders' personal information public by default. Keep in mind the following points.

- SNSs do not offer private space.
- SNSs should not be used for criticizing others.
- SNSs should not be used for making confessions.
- Comments that are posted on SNSs will be difficult to erase.
- Information posted on SNSs will eventually leak out.
- Anonymous comments on SNSs will most likely be tracked down.
- There will be rogues posing as friendly people among SNS users.
- Careless remarks may attract harsh criticisms.

* Twitter, LINE, Google+, GREE, Mobage, and Facebook are all trademarked names of microblog and SNS services.

Protection of Personal Data, Privacy, and Human rights

The Internet, with its various tools, such as email, blogs, and websites, has made it possible for individuals to get across their ideas and opinions globally.

This is indeed a wonderful thing. However, it is also important to understand the risks involved in disclosing information online and to take due care to protect the personal information and privacy of yourself and your acquaintances.

Protect your personal information

Do not disclose data that help identify you. If, for example, perpetrators are able to collect information about your name, address, telephone number, and date of birth, they can use this to commit identity theft.

Think twice about giving away personal details on questionnaires in return for prize draws and gifts, as they may be leaked to third parties.

A simple act of sharing photographs on SNSs can also result in the disclosure of personal information. Photographs taken with smartphones are embedded with GPS coordinates that identify the location the photo was taken. Make sure that you remove the location tags from the photographs you wish to share so that the locations of your home and places you visit, including your friends' homes, remain private. Disclosing such information may result in being stalked or break-ins.

Transmitting information using free Wi-Fi services also poses security risks, as traffic can easily be intercepted by a third party.

Protect personal information of others

You must respect the privacy of others and avoid acting in ways that may violate their human rights.

Information regarding other people should be handled with the utmost care. You should never disclose personal information of others without consent.

Do not read other people's emails. Server administrators will have access to people's email histories. However, bear in mind that snooping on who is communicating with whom is an infringement of privacy.

Do not upload and share videos containing images of people online without their permission. Such actions can be perceived as infringing the rights of publicity (i.e., human rights) of others according to Japanese law.

Researcher Ethics

Students of the Institute are expected to hold high ethical standards as members of the research community.

Never copy and paste someone else's material without proper citation onto your own reports and research papers. It is plagiarism to use other people's material (writings, photos, and charts) without citation. Not only is such an act a breach of copyright, but it is also a violation of researcher ethics.

Online contents should also be used with proper citation. Even when they are in the public domain, ethical standards require that they be properly cited. Information that is available on the Internet may not necessarily be valid. Even if the content seem worth sharing or is written in an authoritative style, do not take them at face value. Always check the sources of information and only cite contents that are reliable.

Data collected in the process of conducting research is essential information for validating research findings. The intentional act of modifying data is called falsification. To tamper with data is to deny the research itself and goes against research ethics.

When research involves handling people's personal information, adequate measures must be taken to protect this information.

Technical information that may be used to manufacture weapons and hazardous materials should also be handled with care. For instance, do not publish on the Internet or disclose to others manufacturing processes and data used in 3D printing.

Protection of Information and Intellectual Property

Words, photographs, and music become legally protected as copyrighted work as soon as they are created. Copyright protection applies not only to printed materials but also to all forms of digital information such as those stored on CDs and published on the Internet. Copyrighted materials cannot, as a rule, be used without permission. There are often conditions attached to their use. The ease with which copying and sending of electronic information can be carried out is no excuse to overlook the copyright of materials. This applies when you use SNSs, file sharing systems, and video sharing websites.

Replication of materials without permission is permitted only in the cases listed below:

- Private use
- Reproduction under certain conditions (e.g., copying in libraries)
- Citation in one's own work, whose contents are comprised mainly of one's own words, with a clear mention of the source of information (See also, P.8, Researcher Ethics)
- Educational use, including citation in exam papers, to the extent that they will not hinder the sales of the original work
- Making a copy of software programs for backup purposes (some software distributed through downloads prohibit making duplicates for this purpose)
- Non-profit performance (For university fetes, the showing of videos may require contracts with video content providers and the use of music may require permission.)
- Reporting of current events

It should be noted, however, that reproducing materials by circumventing copy protection mechanisms is prohibited.

The following is a list of rules and regulations related to copyright:

Copyright of derivative works

Compilations and databases of copyrighted materials are also protected by copyright. Bulk downloading of files from such collections, even when available online, are often prohibited by their terms of use. Make sure that you do not violate the terms of use by using automatic download programs.

Neighboring rights

In addition to the copyright granted to creators, neighboring rights are granted to performers, producers of phonograms, and broadcasters (both wireless and wired). Care must be taken not to infringe their rights as well.

Right to make available for transmission

Make sure that you do not infringe the rights of the owners when copying and redistributing information over the Internet. When posting copyrighted work of others online, you must

gain their permission to make the work transmittable. This also applies to cases when you post videos on video sharing websites.

Moral rights of authors

Through copyright, creators of work are granted two kinds of rights: economic and moral rights. Moral rights give creators the right to (a) maintain the integrity of their work, (b) make the work public, and (c) withhold or make public their name. Never revise contents of a copyrighted work and publish it under the creator's name without permission.

Video and sound trademarks

It is now legally permitted to trademark sounds and videos. Such sounds and videos are protected under the trademark law and must not be used without permission.

File sharing technologies

The use of peer-to-peer (P2P) file sharing software that allows copyrighted materials to be shared without adequate licensing generates the risk of users being embroiled in intellectual property disputes. Furthermore, there have been reports of incidents where personal information and confidential information of corporations were leaked from computers installed with P2P software.

For these reasons, the Institute prohibits the use of P2P software on its network.

Software License

U N P

Users must have a valid software license to install and use a particular software. Installing a software package licensed for one computer onto multiple computers will breach the license agreement and is therefore not permitted. Never take part in software piracy, even if it is at the request of your boss or supervisor.

If it becomes necessary to install a software program on additional computers, make sure that you supplement the licenses accordingly.

Some software products that are used commonly at the Institute are site licensed.

Compliance with Other Laws

Observe the provisions of laws with a full understanding of their intended purposes. Refrain from carrying out the following acts:

- To secretly gain access to other people's accounts and passwords, or to access protected information using security holes in software
- To hack into other people's computers and systems and steal, erase, and/or modify stored information(Punishable under the Act on Prohibition of Unauthorized Computer Access)
- To create malware (Punishable under the Penal Code of Japan [Crime of creation of computer viruses])
- To send or forward unsolicited emails (spam) to others
- To incapacitate web servers by overloading them with a massive number of requests (Punishable under the Penal Code of Japan [Crime of obstruction of business], or the Act on Regulation of Transmission of Specified Electronic Mail if committed as part of a business operation)
- To announce the intention to commit a crime on blogs and other websites (Punishable under the Penal Code of Japan [Crime of obstruction of business, Crime of intimidation])
- To lock laboratory computers or encrypt files and not disclose their passwords to other users for the purpose of harassment
- To send messages persistently (Punishable under the Law on Proscribing Stalking Behavior and Assisting Victims)
- To handle sexual images (Punishable under the Act on Regulation and Punishment of Acts Relating to Child Prostitution and Child Pornography, and the Protection of Children; and the Act on Prevention of Victimization Resulting from Provision of Private Sexual Images [otherwise known as the Revenge Porn Prevention Act])
- To use trademarks of enterprises and/or products on your websites without permission (Punishable under the Trademark Act)
- To illicitly obtain confidential information such as client lists and technical information from enterprises (Punishable under the Unfair Competition Prevention Act)
- To use personal information in ways other than those stated at the time of collection (Punishable under the Act on the Protection of Personal Information, violation of research ethics)

- To divulge findings obtained from a joint research without consent from the collaborating researchers through such means as publishing on the Internet or disclosing to a third party (Infringement of Moral Rights, violation of research ethics)

Judicial rulings may become necessary to decide whether a certain act is illegal or in violation of public policy. You must never justify your illicit conduct by saying that 'other people are getting away with it.' Furthermore, avoid acting in ways that can be misinterpreted by others as being illicit. Protect your integrity by observing the laws, regulations, and other codes of conduct that apply in given circumstances.

Tokyo Tech Employment Regulations

The duties of National University Corporation Tokyo Institute of Technology staff are specified in the Institute's Employment Regulations. The following obligations that applied when staff had civil servant status continue to apply:

- To devote oneself to duty
- To comply with existing laws and regulations, Institute regulations, and orders of superiors in the course of duty

- To protect confidential information acquired during the course of one's duties
- To avoid committing acts that disgrace or damage the credibility of the Institute
- To avoid disrupting discipline and order at the Institute

Using computers for private business during working hours, transferring electronic files containing the Institute's confidential information off campus, and posting messages that have no relevance to one's duties on electronic bulletin boards during working hours are conducts that are in violation of the employment regulations. Failure to comply with the above-mentioned obligations may result in one of the following disciplinary actions: dismissal, suspension, wage reduction, admonition, reprimand, warning, and caution.
Sending emails to colleagues making excessive demands or forcing excessive burden falls under power harassment. Sending emails of the same nature to students you are supervising will fall under academic harassment.

When Trouble Occurs

Notify the Information Ethics Committee when trouble occurs.

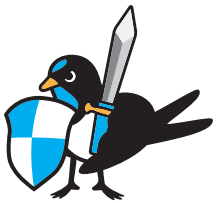
【Contact Information】

Information Ethics Committee

Email：cce@jim.titech.ac.jp

Information Security

Taking adequate security measures is essential to protect data that you and other members of the Institute own from cyberattacks and hardware troubles. The following sections describe the minimum security requirements that you are expected to follow.



Mobile Devices

U P S

Exchanging emails and preparing documents using mobile devices such as smartphones, tablets, and laptops have now become the norm in society. Some members of the Institute may also read messages that have been auto-forwarded from their Institute account on these devices. These small devices, however, are easy to lose, and there is a risk of personal and confidential information being leaked and exploited. In order to minimize this risk, (a) avoid handling confidential information on mobile devices and (b) configure these devices so that authentication is required to gain access.

Data Backup

U P S

The data you own is an important personal asset that you are responsible for protecting. Make sure you regularly back up your data, so that in the event a computer operating system needs reinstalling, your data can still be recovered. Decide on the best ways to back up data for both short- and long-term purposes by taking into account the durability of each storage medium and the risk of storage devices becoming obsolete due to advances in technology (reading data off the medium may become very difficult). One way to store non-sensitive data is to use a reliable online storage service.

Countermeasures against Viruses

The threat of computer viruses is an ever-growing concern not only for PCs but for various mobile devices as well. Never underestimate the harm they can cause — some viruses can destroy data. Worst still, they can spread over the network without you realizing and destroy data on your friends' computers.
To protect your PCs from viruses, install a virus scanner in each computer and routinely update the scanner so that the latest virus pattern file gets used. Taking these little steps to safeguard your computers on a daily basis will go a long way in protecting your information.

Despite their effectiveness, virus scanners do not provide complete protection. Computers will still be vulnerable to new viruses for which antivirus software manufacturers have not yet issued an update. Targeted virus attacks are on the rise too. This is where attackers try to infect computers of a certain individual or organization. They may come in the form of suspicious emails, email attachments, or software that is downloaded when you click on a link to dubious websites.
It is therefore important for users to practice the following safety habits:

- Do not open emails from an unknown sender.
- Do not click on any links or open attachments of odd-looking messages, even if the sender is someone you know.

Simply put, if you think something isn't quite right, assume that it's not. If you need to confirm the legitimacy of an email, try contacting the relevant organization or individual using a valid contact address or by phone.

Computers can also become infected by a virus simply by visiting websites. Refrain from visiting louche websites for entertainment.
Do not install freely available software from unreliable sources. You may risk infecting your computer with spyware, a program that covertly gathers data, such as your personal information and computer activities, and sends them to another entity.

Security Updates

Always install the latest security updates for the operating system (OS) and application software installed on your computers. Procrastinating and avoiding the hassle of updating your software will put you at risk of irreparable damage. Make it a habit to check if installing security updates is necessary when you switch on your PCs.

Always upgrade to a new OS before support is withdrawn from the version in use. Remember that security updates will not be provided for OSs that are no longer supported.

Password Management and Hacking Countermeasures

Passwords are like keys to locks that protect information systems. If your password gets into the wrong hands, it could be used to access information systems with malicious intent. Pay attention to the following points regarding password management:

- Do not tell your passwords to anyone, not even to your friends. Avoid keeping a memo of your passwords close to the computer.
- Use strong passwords. Make them long and unpredictable.
- Avoid passwords with number sequences and repetitive characters.
- Be on the alert for phishing, where fraudsters try to trick you into disclosing sensitive information. They may masquerade as IT administrators and make a request for you to log onto a fake website in order to verify your account on a newly updated system. System administrators never send messages with such a request.

Computers are not the only electronic devices that require password protection. Other forms of devices that can be connected to a network, printers and network cameras for example, must also be set with strong passwords. Failure to change their default settings will make these devices accessible by others via the Internet and may result in information leakage. (Refer to instruction manuals for the setting of passwords.)

The development of a diverse range of services including social network, free email, and cloud services that are interconnected with each other have made the Internet ever more convenient. The downside to this is that users are now depositing various signposts that lead to sensitive information all over the Internet. If a single set of ID and password is used to access a number of services, hackers may be able to piece together sensitive information such as a password to an important email account. In order to avoid this kind of risk, do not use a common ID or password for different services.

Attention should also be paid to the risks involved in using the various cloud services that are now available. Do not use cloud service providers, especially those offering free service, to upload important or sensitive data belonging to you or the Institute. If you are going to use cloud services, make sure that you are prepared for the occasional service outages.

File Sharing and Network Management

U N P S

Do not share your PC with others, even with friends or family, as this may compromise the security of stored data.

Do not share the same account ID or password with others. You should not use the same password for or recycle passwords amongst multiple services either.

Also, cloud service accounts (such as Google accounts) that allow users to access various services with a single sign-in can leave an opening for others if you forget to sign out before closing the browser. Always remember to sign out once you have finished using these services so that people who use the same computer may not access your account.

Pay attention to file sharing settings so that files are not shared unnecessarily. When you create a new file or folder, always check its sharing settings. In order to maximize security, it is also effective to set up firewalls on individual PCs as well as on routers. Make it a rule to keep ports that are accessible from the Internet closed unless they are necessary.

System Trouble

It is beyond reproach to deliberately perform acts that destruct information assets and systems. However, it is important to stress that an operation mistake or an unmalicious act performed out of curiosity may still cause system trouble or damage to information assets of others. Should such an incident occur, notify the system administrator immediately and try your best to contain the damage. Do not attempt to hide the incident.

Unauthorized Access and Data Leakage

If you experience a security incident, such as an unauthorized access or information leak, request help. Contact the relevant system administrator and Tokyo Tech Computer Emergency Response Team (Tokyo Tech CERT) immediately. (Tokyo Tech CERT is responsible for maintaining the security of the Institute's information systems.)

【Contact Information】

Tokyo Tech CERT

Email：contact@cert.titech.ac.jp

Q&A

Q. Connecting a Personally-Owned Computer to the Institute Network

Am I allowed to connect my own computer to the Institute network? If so, what points should I pay attention to?

A. Consult the network administrator of the laboratory you belong to. You may also connect to the on-campus wireless LAN through the access points available at various public spaces on campus, such as the campus cafeteria. Please make sure that your computer is free of viruses. The Institute has, in the past, had its computers infected with viruses. In one case, it was the student's personally-owned computer that was the source of infection. Also, pay attention to your PC's network sharing settings and firewall settings.

Q. Accessing Tokyo Tech Portal

Why is accessing Tokyo Tech Portal such a cumbersome process?

A. Access to Tokyo Tech Portal requires either an ID and password and matrix authentication or public key infrastructure and PIN authentication. This strict two-step authentication process is necessary to protect the Portal from unauthorized access by outsiders.

Q. Installing Software Licensed to the Institute on a Personally-Owned Computer

Can I install software that is licensed to my laboratory onto my own computer?

A. This must be considered in terms of (a) software license agreement and (b) justifiable use of the Institute's resources. In terms of software copyright, as long as you are not in breach of the license agreement, there should be no problems. However, as with other purchases, what is bought by the laboratory should be used for the purpose of carrying out tasks directly related to the laboratory.
Installing laboratory licensed software to a personally-owned computer can be perceived as misappropriation, and is therefore discouraged.

Q. Document Retrieval

A friend asked me if I could retrieve some documents for him from the databases and electronic journals that are accessible from the Institute online. He belongs to another university. Can I do this?

A. The databases and electronic journals are licensed resources whose use is restricted to the Institute's faculty and students. Using these resources other than for your own research and education will be in breach of the license agreements. If a breach of contract is discovered, the provider will suspend access to their resources for the entire Institute community. You must not, under any circumstance, retrieve information from the licensed resources for another person's use.

Q. Downloading from Databases

Are there any other restrictions that I should be aware of when downloading data and documents from database providers and journal websites?

A. Downloading large volumes of data for research and educational purposes require the provider's approval. If you need to do so, please contact the Institute Library staff. The Institute has, in the past, experienced suspension of service by providers as a result of bulk downloading.

Q. Keeping a Copy of Security Updates

Our network recently became contaminated when a visitor's virus-infected computer was connected to the network. In response to this, we thought about setting up a policy banning the connection of computers that are not properly protected with security updates and virus definition files. Not being able to connect some of our visitors' computers to our network is an inconvenience, however. There is also the conundrum that, without online access, it would be difficult to get a computer's security up to date. So, we are currently considering compiling a security update CD that visitors can use to make their computer safe enough to connect to our network. Is this allowed?

A. If you cannot confirm that a visitor's computer is properly protected, do not connect it to the Institute network. Try other methods. For example, allocate an Institute-owned computer to the visitor and have the necessary data transferred to it.

Q. Disclosure of Own Paper

Can I upload papers that I have written for conferences and journals on my own website?

A. It is normal practice for researchers to upload papers they have written on their personal website once they have been submitted to journals and international conferences. However, some academic societies have strict policies regarding this issue. Even when the copyright of a paper belongs to the author, societies may still restrict papers from being published anywhere other than in their journal (irrespective of whether the version to be posted is the journal's accepted version or not). Furthermore, it is important to consult the society on the conditions that apply once your paper becomes accepted. (Faculty and students should also refer to the operation guidance for T2R2.)

Q. Disclosure of Research Progress

Can I disclose the progress of my own research on the Internet?

A. Consider the following points very carefully before disclosing your progress on the Internet. It might be the case that the research you are conducting is based on advice given by your supervisor or contains ideas and unpublished research findings of your colleagues. By revealing your progress, you might be disclosing ideas of your supervisor or colleagues who may not wish to have them disclosed. There is also the risk of someone submitting a paper based on the information that you have posted before you yourself have had the chance to publish yours. If this occurs, proving that your research findings were plagiarized will be difficult. Be aware of the risks. If you are a student, you should consult your supervisor first.

Q. Responsible Use of the Institute's Computing and Networking Resources

I recently took part in an online discussion about issues concerning university reform, and raised some points as well. Will I be penalized for this?

A. Your action cannot be considered as part of education and research activities, but it came out of concern for the Institute's future as a member of the Institute community. Furthermore, computers and networks are now an established part of the information infrastructure and support the members of the Institute to carry out their duties. Your use of this medium may not be problematic in that respect. However, the point at issue here is whether participating in such discussions during working hours is acceptable conduct or not.

Q. Can Telling Facts Be Considered Defamatory?

I once shared details about a friend of mine on my blog and to subscribers of a mailing list — details he did not want disclosed. It was not meant to be defamatory. I thought I was simply stating a fact, but my friend does not see it that way.

A. Everyone knows that spreading false rumors is inadmissible. Less known is the fact that disclosing the truth can also be defamatory in some cases. (And real acts of defamation often are based on truths, don't you think?) Please be aware that disclosing the truth can also lead to a case of defamation or invasion of human rights.

Q. Email Etiquette

A friend of mine once replied to my email strongly refuting my statement. This would not have been a problem if he had only sent his reply to me. However, he chose to send the message to all subscribers of a mailing list without my consent. Is such behavior permitted?

A. This may be perceived as strongly criticizing someone in public, and hence constitute defamation. Always gain the permission of the author before forwarding the contents of an email to a third party.

Q. Copy Protection

Would copying contents of CDs and DVDs by circumventing copy protection mechanisms using a program be considered an act of copyright infringement?

A. According to Article 30, paragraph 1 of the Copyright Act ("reproduction for private use"), an individual may duplicate a copyrighted material if the copy is intended for personal use or family use or other equivalent use within a limited scope. However, this does not apply when copies are made while knowing that replication is only possible by circumventing copy protection (Article 30, paragraph 1, item 2).

In the case of the question you posed, since you are fully aware of your action to circumvent copy protection, the exception of "reproduction for private use" does not apply. In conclusion, your actions will be deemed an infringement of copyright.

Q. Use of a Program by Multiple Users

I want to establish a client-server system where the client computers execute programs that are stored on the server. What legal requirements must I adhere to?

A. Under the Copyright Act of Japan, copyright owners are granted the Right to Make Available for Transmission and Right of Reproduction. This means that in addition to gaining permission to duplicate the program, you will need to gain permission to make the program transmittable from the copyright owner. You will find that many license agreements require users to expressly gain permission of use of the software in this way.

Q. Use of Electronic Dictionaries and Books by Multiple Users

I want to store copyrighted digital publications (such as a digital encyclopedia) on a server within the Institute's network, which can be accessed by multiple client computers. What are the legal issues regarding this?

A. Even if the digital encyclopedia has been licensed to be installed on a computer, some publishers restrict its access by a large number of client computers.
In addition, copyright issues will arise if servers store data of scanned books.

Q. Cyberthreats

What kind of threats to our computers should we be careful of?

A. One source of threat is malware. This kind of software might covertly gather sensitive information or take unauthorized control of a system. Examples of malware include computer viruses, worms, and trojan horses. Another form of threat is denial-of-service attacks where access to a web server is overloaded, leaving it unable to serve legitimate users.

To prevent computer systems from being disrupted, it is vital that the security systems are kept up to date.

Q. Countermeasures against Hacking

How can I prevent hacking?

A. First, make sure that your computers' operating systems are up to date with all known security holes fixed using patches. Security holes are flaws in software programs and are prevalent in large and complex operating systems. Vulnerabilities found in OSs are perfect gateways for crackers to access computer systems. Second, check that the network to which you connect your computers are guarded with a proper firewall and that your computers have been configured with firewalls as well. Third, guard against malware by constantly running antivirus software.

Q. Defamatory Posts on the Internet

I found a blog containing defamatory posts about me. What actions can I take?

A. You can request the provider of the blog service to take down the harmful contents. These cases, however, can be difficult to resolve alone. You may want to seek help from the Legal Affairs Bureau or the police by forwarding a claim of human rights violation or defamation. When a site contains a significant amount of harmful content, it is possible to prevent search engines from showing the site in the search results, but the procedure is complex. You will need the help of professionals such as an attorney. Free legal consultation is also available at the Japan Legal Support Center.

Japan Legal Support Center
http://www.houterasu.or.jp/index.html

Appendix: Relevant Links

Tokyo Institute of Technology Information Ethics Committee

http://www.titech.ac.jp/rinri/
(An online version of this handbook can be found here.)

Email：cce@jim.titech.ac.jp

Tokyo Tech Computer Emergency Response Team

http://cert.titech.ac.jp/

Email：contact@cert.titech.ac.jp

National University Corporation Tokyo Institute of Technology Information Ethics Policy

http://www.jyoho.jim.titech.ac.jp/kik_sui/security/policy_1.pdf

National University Corporation Tokyo Institute of Technology Information Security Policy

http://www.jyoho.jim.titech.ac.jp/kik_sui/security/policy_2.pdf

Reporting of security incidents

http://www.jyoho.jim.titech.ac.jp/kik_sui/security/index.html#higai

The Institute is required to inform the Ministry of Education, Culture, Sports, Science and Technology of all incidents of security breaches. If you discover any security breaches, please fill in and submit the security incident report form (a Japanese form is available from the above web page) to the Information Infrastructure Division without delay. When sending the initial report, use the form to give details of what you already know at that point in time. Do not delay reporting to gather enough information to complete the form.

Incidents must be reported to:

Information Planning Group
Information Infrastructure Division
Research Promotion Department

Email：kib.kik@jim.titech.ac.jp

Information Ethics Expert Committee Working Group

Chairperson:	Associate Professor Hironao Kaneko
Vice-chairperson:	Associate Professor Ken Wakita
Members:	Associate Professor Ken Ishikawa
	Professor Minoru Sakurai
	Professor Toshiya Itoh
	Professor Masahiro Yamaguchi
	Professor Osamu Watanabe
	Professor Haruo Yokota
	Professor Masahiko Tomoishi
	Associate Professor Katsuyoshi Iida
	Associate Professor Satoshi Matsuura
	Associate Professor Reiko Sato
	Associate Professor Gyoubai Sen
	Toyoka Akitomo, Head of Public Relations and Outreach Division
	Noboru Tanaka, Head of Student Division
	Yasuo Matsubara, Head of Information Infrastructure Division
	(The members list is in no particular order.)

Staff responsible for administrative tasks:
Takashi Kodera, Hiroshi Moriya, Information Infrastructure Division

Guidelines for Information Ethics and Security (2nd Edition)

First edition published April 1, 2005
Second edition published April 1, 2016
Edited by the Information Ethics Expert Committee Working Group
Published by Tokyo Institute of Technology

201610.2000 / gram inc.