Guidelines on delivering information

Center for Information Technology, Kansai University

1 Purpose of these guidelines
It is certainly essential to deliver information over the Internet. On the other hand, information delivery that involves violations of various rights is likely to cause the university to decrease productivity and lose the trust of society. When delivering information to post personal messages, whether it is from the university's domain or from a URL that belongs to a personally contracted Internet service provider (ISP) or on private SNS (e.g., Twitter, Facebook), you are often considered a public figure who belongs to the university. You need to be careful when doing so. The purpose of these guidelines is to reduce related risks, protect information assets, and specify what is necessary for users to accurately, safely, and securely disclose various types of content and information over the Internet.

2 Intended audience for these guidelines
The intended audience for these guidelines includes the members of the university who deliver information over the Internet.

3 General precautions regarding delivering information on the university network
When delivering various kinds of information, you shall observe not only relevant laws and regulations but also the SINET terms of use and relevant university rules.
Also, you shall not do anything that would contravene public order or morality or transgress socially accepted ideas even when delivering information.

Here is an excerpt of the SINET participation provisions for your reference. For the entirety of the content, see the SINET page (http://www.sinet.ad.jp/).

Article 6 (provisions to observe upon participation)
The participant shall observe what is specified in the following provisions:
1) Do not use the network for purposes other than education or research, or management tasks to support them.
2) Do not use the network for commercial purposes.
3) Do not violate communication secrets.
4) Do not use the network in a way that interferes with network operations.
5) Make utmost efforts to prevent unauthorized actions against the network and computers.
6) Other provisions the director stipulates separately

You shall keep in mind that while delivering information over the network brings many benefits, various dangers and risks are involved. You should be fully aware of the meaning and danger that is involved. This is the responsibility of those who deliver information. You should keep in mind that the world of networks is based on the principle of self-responsibility, just like the real world.

(1) Observing intellectual property rights such as copyrights
Do not violate others' intellectual property rights. Violations of copyrights are likely to occur especially when creating or publishing Web pages. We need to take extra care when doing so. Copyrights exist for works created by others. As a general rule, do not post content created by someone other than yourself without approval.
(2) Observing portrait rights and publicity rights
Do not violate others' portrait rights or publicity rights. People are considered to possess their respective portrait rights as their personality rights. You shall take extra care when posting photos with the faces of others in them. As a general rule, do not post such photos without approval.
(3) Prohibited delivery of information that causes others trouble
When delivering information over the network, do not deliver information that causes others trouble. Information that causes others trouble includes:
1) Content that defames people
2) Content that contains information that might violate others' privacy
(4) Precautions when posting information on research achievements and interim progress
When posting information on research achievements and interim progress, make sure that there are no problems that would arise when disclosing them. The same applies to data acquired through experiments.
(5) Handling company names and logos
When posting the logos of sponsor companies at academic meetings or symposiums, discuss the

matter with the university and relevant companies in advance.

(6) Risks associated with posted facial photos

When posting your own portrait photos, you should fully consider the risk of exposing your face.

(7) Other (prohibited delivery of information that goes against public order and morality)

Do not deliver information that goes against public order and morality or is harmful, not to mention illegal information.

4 Precautions when disclosing materials from digital archives

When disclosing materials from digital archives such as classic materials on the Internet, make sure that use of such materials has already been permitted as far as rights go.

5 Observing various usage regulations and prohibited use other than use for intended purposes

Those who deliver information shall observe the provisions and terms of use regarding relevant information systems and services, in addition to these guidelines. They shall not use such systems or services for purposes other than purposes of use specified by the university and purposes specified by SINET, either. The university's information system and SINET are provided for purposes of encouraging education and research, performing tasks, and providing support. This is why those who deliver information need to be distinctly aware of what is official and what is private and take extra caution not to disclose information that is irrelevant to or inappropriate for the purposes for which these systems and services are provided. Typical examples of out-of-scope use include the use of the university's information system for commercial purposes to earn profits rather than for research purposes.

6 Ensuring system safety

(1) Ensuring security

Be sufficiently sure to ensure security when designing a Website. In particular, bug-fix patches should be applied to operating systems and various software applications to keep them consistently up-to-date. The same applies to outsourcing Website design work.

(2) Precautions about CGI, use of SSL/TLS

1) The security level is lowered with the use of CGI on a Website. It is recommended that CGI not be used.

2) Be sure to use secured communications such as SSL/TLS on pages that require the entry of passwords and personal information.

(3) Precautions about hidden directories

Do not store information that should not be disclosed even in hidden directories.

(4) Precautions about public bulletin board systems (BBS)

Public bulletin board systems (BBS) can cause difficulties such as violations of various rights, as anyone can post anything freely. It is desirable not to set one up unless there is some special reason for so doing. If you set up a public bulletin board system (BBS) on a laboratory or personal server, it is recommended that you use password authentication to actually limit the number of users who can use it.

(5) Ensuring sufficient server capacity and network resources

When setting up a server to publish a Website, the machine and network used for the purpose should accommodate sufficient access.

7 Scope of responsibilities of a Website or BBS administrator

The Provider Liability Limitation Act regards Website or BBS administrators as "Specified Telecommunications Service Providers." Those who manage Website or BBS content bear the responsibilities and duties specified by the act. They shall take extra care.

Additionally, if obvious violations of rights are observed on any server or in any network at the university, the Center for Information Technology shall have the information that violates rights removed as quickly as possible or remove it using a separately specified format.

(An example of a warning letter)

WARNING

YYYY   MM   DD

Dear_____,

Center for Information Technology, Kansai University

    We have found that distribution of the following information posted on your Website has resulted in violations of rights of others. Also, we have found it difficult for the target of the said violations to take preventative measures against such violations, considering various factors in a comprehensive manner.
    Therefore, you are hereby requested to take immediate measures to prevent the said information from being sent. If measures to prevent the content from being sent are not taken by DD, we will take the liberty of removing it.

Location in which the content is posted:
    *Specify information necessary to identify the URL and the said information.
Posted information:
    *Specify the type of information that violates rights.
    Posting information that goes against privacy, violates the intellectual property rights of others, and the like.

---

8 Precautions when delivering information on social media
    If your social media profile includes information to the effect that you are a Kansai University student, or if this information can be found by searching even if it is not disclosed, the same degree of caution is required as you would exercise when delivering information from within the university, in order not to impair the university's trust. There is also the possibility that you would end up disclosing that you are a Kansai University student because of your comments.

9 Contact for these guidelines
    If Web administrators need to cope with emergencies or take measures beyond the scope of these guidelines, they shall contact the Center for Information Technology for support and instructions.

Supplementary provisions
1. These guidelines become effective on November 6, 2019.