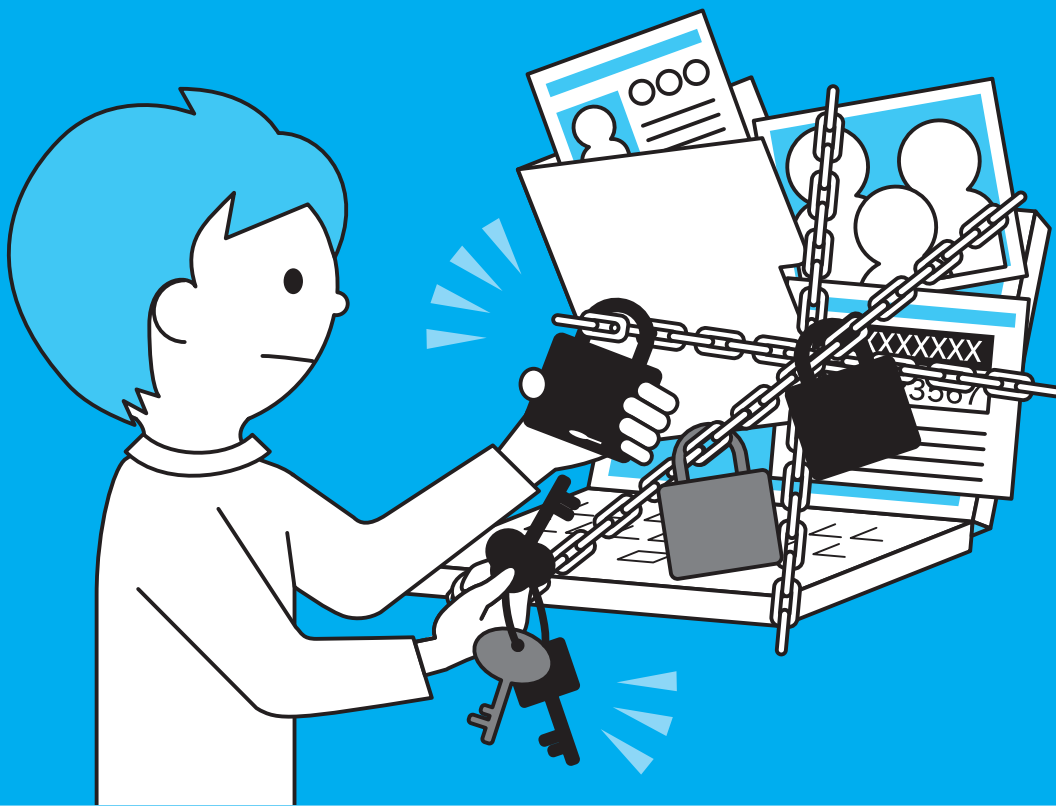# To All Students

The key principles are:
"Protect your personal information by yourself"
and "Do not infringe on personal information and copyright of others."

Information Security for You

早稲田大学

WASEDA University
早稲田大学

Case 1 — I submitted someone else's copyrighted material I found on a web site as my report and I didn't indicate the source.

To quote someone else's work and to submit it as your own is a violation of the Copyright Act and considered "plagiarism (theft)." Citation is permitted as long as it strictly meets the requirements for citation, such as separating the quoted part from the main text and indicating the source of the citation. If you fail to do so, it is regarded as an illicit act called plagiarism. Any student who is found to be engaged in such illicit act is subject to severe punitive measures by the University, such as, disqualification of enrollment in all courses in the semester and suspension from the University.

All students must be aware of the rules of quoting someone else's work when submitting reports. The following acts, for example, will be regarded as plagiarism:

👉 To obtain someone else's work from a Web site, a book or a report, and submit it as your own after modifying the words partially or changing the order of the words.

👉 To submit a report (essay) obtained from a report (essay)-sharing web site (service) as your own writings.

Case 2 — I opened an attached file or clicked a link with an email that comes from an unknown sender.

There is a risk that a computer virus is attached to the file or that an email contains a link to a fake website. These viruses and fake websites would steal confidential information, corrupt data and even attack on other PCs. When it happens, please remove LAN cable from the network or disconnect the network connection if you are using Wi-Fi. Please contact Helpdesk immediately and ask directions.

Case 3 — I posted inappropriate information on social media such as Twitter, Facebook, LINE and the university page such as My Portfolio.

Please keep in mind that information you post on the Internet is not only accessible to the general public of various backgrounds and locations, but also it is impossible to delete completely from the internet. This holds true regardless of whether you are logging on to your business or to your private account. (Note that information may be reproduced even if it is designated to be accessible only by a selected few.) Remember that there is no complete assurance of anonymity on the Internet and that even information imparted by an individual could provide the basis for the evaluation of the organization. Be fully responsible for your conduct and do not let your guard down when using social media and social networking sites. There have been many cases of inappropriate posts, such as unauthorized disclosure of information on encounter with famous people or friends' private information, illegal or inappropriate behavior by the person making the post, and so forth. It is needless to say that there is no excuse for illegal or dishonest behavior itself, including cheating, driving under the influence of alcohol, etc., but the negative effects may be exacerbated greatly when these behaviors are exposed on the Internet, and the information may prevail in society much more deeply than the individual expects. Inappropriate use of social media by students has caused enormous problems in the past and in some cases resulted in corporate enterprise canceling offers of employment to the students involved. The same applies to the "MyPortfolio" system, so please exercise caution when publishing information on your portfolio as you are responsible for keeping your information safe. Should you find yourself in any trouble, please consult the administration office of the University.
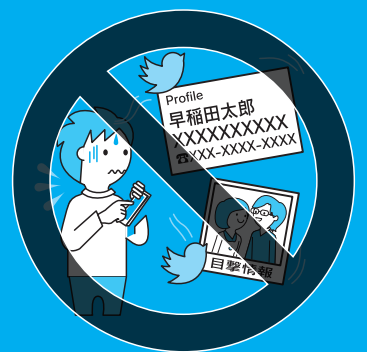
Trends Related to Information Security

Protection of Personal Information

The term "personal information," used here, refers to any information that may be used to identify an individual.

The main stipulations of the Act on Protection of Personal Information are: (1) clarity about the purposes to which personal information is to be put and restrictions on the use of personal information for purposes other than that for which it has been collected for; (2) the fair collection of personal information and notification of the purposes for which personal information is processed; (3) assurance of the accuracy of personal information and security measures; (4) supervision over workers and contractors and restrictions on the disclosure of personal information to third parties; and (5) disclosure, revision, cease of use, etc. of personal information at the request of the individual concerned.

Copyright

Due to revisions to the Copyright Law enacted on April 28, 2020, it is now possible to use third-party copyrighted materials without express permission when streaming content online if used within class. However, this is under the premises of "Within limits as deemed necessary" and "No undue harm to the copyright holder's interests", so please exercise caution and engage in appropriate usage.

Revisions to the Copyright Law enacted on January 1, 2021 **expanded the restrictions on downloading copyrighted materials illegally uploaded online (Infringing Content) from only music and images to all copyrighted materials (including manga, magazines, fiction, photographs, academic articles, computer programs, etc.).** Repeatedly or continuously downloading infringing content of copyrighted materials which are being officially distributed for profit may result in criminal punishment (Up to 2 years imprisonment or 2 million yen fine (or both)). Downloading copyrighted materials such as music or images from illegal websites is strictly prohibited. Please refer to the Agency for Cultural Affairs website, etc. to acquire accurate knowledge.

Initiatives at Waseda University

Initiatives for Protection of Personal Information

👉 **Reference URL** 1

With the aim of promoting protection of personal information, Waseda University established the "Personal Information Security Rules" on May 26, 1995. Waseda University protects and manages the personal information based on the the rule and related law and regulations.

Initiatives for Information Security

In September 2002, the University established the "Waseda University's Information Security Policy" (hereinafter referred to as "the Policy") which specified minimum rules to be complied with when information is handled via the computers and network systems at the University. The Policy provides that all users of the services offered by the University have the responsibility to observe the Policy and must not engage in any unauthorized access, alteration, reproduction, destruction, leakage, etc. of information assets both within and outside the University, even if it is unintentionally.

Furthermore, the University established "Regulations on Information Security measures" on January 2012, and is taking some measures to meet security requirements.

Initiatives for Protection of Research Information

"Security Guidelines for the Protection of Research Information" was established in January 2021, introducing "the proper mindset regarding security measures" and "specific examples of security measures" that are useful in protecting important research information from threats such as leakage, falsification, and loss.

Initiatives for Protection of Copyright

In addition, the University released the "Guidelines for Creating Contents Used on the World Wide Web by WIND (Waseda's Internet Domain)" in November 2003, with the aim of promoting proper use of the information network among WIND users in accordance with legislation and social norms. Moreover, in order to raise awareness of this issue, the University issued the announcement on the "Handling Written Materials in a Web Context for Education and Research Purposes" in March 2004.

Cautions

Cautions Concerning Protection of Personal Information

In June 2015, highly sensitive personal information in the possession of the University was found to have been unintentionally released. Loss or theft of laptop computers and USB flash memory devices containing personal data has also been reported.

Many other accidents involving leakage of personal information have occurred. For example, a computer storing personal information was stolen from the owner's house by a burglar, and a bag for carrying a laptop computer and a USB flash memory device was stolen while the owner moving on a train. It has been also reported that while a person working on some data containing personal information at home, the computer leaked the personal information through file sharing software, and it turned out that the computer had been infected by virus. Common to these cases is that documents (paper-based / data) and storage media containing personal information are taken out of the campus without taking appropriate care.

There have been increasing cases of e-mails being sent to the wrong recipients. Extra caution is advised in order to avoid unexpected abuse of potentially sensitive personal information released unintentionally.

In order to prevent for someone from cracking your password, set yourpassword with more than 8 characters and mix of upper and lower casealphabetical and numeric characters. Do not use the same password in multiple PCs and the systems. 👉 **Reference URL** 2 3

Please observe the following points when handling documents (paper-based / data), storage media, etc. containing personal information.

(1) Do not take any documents (paper-based/data), storage media, etc. containing personal information out of the University incautiously without appropriate care.
(2) Store documents (paper-based data), storage media, etc. containing personal information in places not accessible to a third person.
(3) Use laptop computers, USB flash memory devices, external hard disk drives, etc. with security features (encryption, user authentication, etc.) and complete the encryption process when storing the data. Do not use file-sharing software such as Winny, WinMX, and Share, as they can cause virus infection and information leakage.

Social security number "My Number" is extremely sensitive personal information. If the payment was made to you by the University, for instance if you did a part time job for the University, the third party vendor may ask you to provide them with your social security number (My number). There may be a risk someone would try to gain access to your social security number (My Number) fraudulently. Please refer to" My Waseda" for how to provide your social security number to others. Do not keep/ notate someone elses' / Friends' social security number (My Number) information.

Cautions Concerning Computer Virus Infections

👉 **Reference URL** 4

It is important to install anti-virus software to prevent computer virus (hereinafter "virus") infection. But installing anti-virus software alone is not enough. Please keep your virus definition file updated to the latest version in order to protect your data from new virus. In addition, please collect information regularly via the Internet, etc. to check vulnerabilities (security holes) of all software you use, including OS such as Windows and Macintosh. If security patches are released, please install them and update the software programs as soon as possible. Reports on vulnerabilities that require immediate actions are issued by the Information-technology Promotion Agency (IPA), IT Security Center Section. For more details, please refer to the reference URLs below.

Waseda University also provides an anti-virus software service for free available solely on its campus network. If you have not installed any anti-virus software, or if you are using expired anti-virus software, please consider using this service.

Cautions Concerning Appropriate Use of Licenses

Abuse of software is strictly prohibited. The abuser is subject to extremely serious punishment decreed by law, defined as "up to ten years in prison and up to 10 million yen in fines." No exception applies to university organizations for research and education. As recently as the end of fiscal 2010, a national university corporation paid an enormous amount of money to settle a software copyright infringement claim made against it.

In addition, as in the examples below, there is a risk that some users may be unintentionally committing abuse of software.

Examples of software abuse
・To borrow software bought by someone else in your laboratory/faculty room or student club, and install it on your own computer
・To buy and use an illegally-copied media
・To download and use illegally-copied software from the Internet or P2P software
・To download software from an suspicious website or an unauthorized website and use it

In particular, software bought for groups such as laboratories/faculty rooms and student clubs must be used under appropriate management methods and procedures. The following is an example of simple method for license management.

License Management Method (example)
(1) Choose a person who will be responsible for software management.
(2) Store the license certificate and the contract obtained at the time of software purchase in a safe place.
(3) Create a License Management Register with the following categories.
　・Name of the purchased software ・The number of installations allowed
　・Date of purchase and duration of software use
(4) Create a register of the devices in which the software has been installed. Include the following categories in this register (as a Software Management Register).
　・Name of the software 　・Name of users and name of devices in which the software has been installed
　・Date of installation/uninstallation 　・Date of purchase and duration of software use
(5) Compare the License Management Register with the Software Management Register and confirm that the number of computers/devices using the same software does not exceed the number of the purchased software licenses.