User Guideline for Information Network System of Osaka School of International Public Policy

1 Introduction

All equipment for computer networking and telecommunication, including all operating softwares, of the Osaka Daigaku Information Network System (ODINS) are intended for the use of research and education. The daily operation and maintenance of the System are carried out by Central Office for Information Infrastructure. Eligible users for ODINS service should observe this Guideline to sustain the full operation of ODINS which is a national property. In addition to academia, the users should also contribute to industry, general public, and especially local communities through their research and educational activities. All faculty, staff, students, and other relevant personnel of this university are therefore expected to have clear understanding of the above principles. The present Guideline is formed accordingly in order to achieve smooth operation of ODINS with high efficiency.

2 Network between ODINS and external terminals outside the University.

The links between the University and external computers are connected by wideband communication network which is not only connected to academic networks, but also to those for commercial use. Various networks have different scales and functions. For example, to look a webpage of a US university, several networks are needed to transmit the data. It should be noted that the capacities of external networks are smaller than those within the ODINS. And even for the same amount of data, the workload for small capacity networks is heavier than that for ODINS. Therefore, transmission of unnecessarily large amount of data should be avoided as much as possible. Although it is possible to access networks worldwide via ODINS, users should be aware that each network has its own operation regulations and every network needs the support of many people.

3 Inappropriate behaviours when using ODINS

Physically, ODNIS is a connection among individual computers. However, it is human who use the connection. The users of ODNIS should therefore follow the common moral and ethical principles. Inappropriate behaviours, such as the following, are prohibited when using ODINS.

- behaviours against the law or against public regulations and orders;
- behaviours inappropriate for the research and education of the University; and
- behaviours affecting ODINS operation

In addition, for the safe and smooth operation, ODINS records the working history of all users. Warning is issued for behaviours hereby forbidden. More serious measures, such as

restrictions on use, notification to affiliated departments, reporting incidents to Network Center steering committee, and publication of name and penalty, are taken for repeated offenders.

3.1 Behaviours against the law or against public regulations and orders

The applicable laws governing ODINS are relevant domestic laws, not international laws or Japanese laws for international issues. The particularly relevant laws are all individual articles for copy right and intelligent property (such as prohibition of inappropriate access), criminal laws, civil laws, commercial laws, etc. In addition, in the case of foreign implications, relevant laws of other counties may be applicable. In addition, behaviours that are not prohibited by law but are generally condemned by society should also be avoided when using ODINS. The following activities are not allowed in the use of ODINS.

(1). Violation of basic human rights - Basic human rights must be respected under any circumstance, not only when using networks;

(2). Publication and propagation of insulting materials – The Japanese Constitution states the respect of basic human rights. Therefore, it is forbidden to communicate insulting materials on race, sex, religion, etc. via ODINS network system;

(3). Inappropriate personal attacks and anecdotes – Such behaviours may lead to criminal law suits in general. It is prohibited to use network system to publish and propagate materials of this nature;

(4). Invasion of privacy – The personal information of ODINS users is protected. Users should respect the privacy of others. Without permission, personal information and private matters are prohibited to be made public;

(5). Hack into unauthorised materials and use of computers and communication equipment without pre-authorization – It is prohibited to use any equipment of the ODINS without authorization, either internally within ODINS or between ODINS and external computers. Hacking from ODINS into other networks may result in not only the total interruption of all external connections from Osaka University, but also possible problems of international nature. In addition, it is strictly forbidden to access transmitted data in the networks without permission;

(6). Violation of intelligent property – Intelligent property is the protection of human creativity. Recognition should be shown to all kinds of intelligent property such as paintings, novels, softwares, designs, etc. Unlicensed copy and modification of any kind are prohibited. For example, without permission, articles, pictures, photographs, videos and music published in

books, magazines, and websites are not allowed to be copied or modified, in order to be further published in other webpages or to be submitted elsewhere. Such action is not only the violation of copyright, but also the infringement of trademark and other commercial laws. It should be particularly mentioned that the photographs of celebrities are protected by the relevant laws under copyright. Finally, it is illegal to copy softwares and/or data from other universities without proper prior agreements;

(7). Publication and propagation of pornographic materials – Pictures, videos, and audios of pornographic nature are prohibited to be posted on ODINS, nor is any connection to such materials allowed;

(8). Abuse of authorization – Users may not allow other people explore their authorized use (codes/passwords and accounts) of ODINS, with or without compensation. All users are responsible for appropriate maintenance of their accounts. Renting login or storage space to others is prohibited. Conversely, users should not use other logins than their own to send email and web information, or to use e-display; and

(9). Psychiatric and harassing behaviours – It is prohibited to send harassing messages to individuals using ODINS. Large amounts of useless emails are also forbidden.

3.2 Behaviours inappropriate for the research and education of the University

ODINS is established to serve the research and education of the University. Therefore, use of ODINS for non-research or non-educational proposes may be restricted. The following uses should be strongly discouraged.

(1). Activities of political and/or religious purposes – Because ODINS is a national property, it should not be used to provide assistance to any political party or religious group;

(2). For-profit activities – Any website and email of commercial for profit nature are prohibited. This includes the information and materials for night classes; and

(3). Storage of data for non-research and non-educational use – personal storage space and website should not contain data irrelevant to research and education

3.3 Behaviours affecting ODINS operation

Any behaviour that can cause physical damage to ODINS is obviously prohibited. In addition, activities that can result in adverse impact or inconvenience to other users should also been strongly discouraged. These include:

(1). Change, or attempt to change, any physical part and/or peripheral machinery of ODINS;

(2). Change, or attempt to change, any software structure in the network;

(3). Install and use, or attempt to do, any software that may affect the normal operation of ODINS; and

(4). Send necessarily large amount of data, affecting network function.

4 Network well-being

For the well-being of the network, the following issues should be considered, although they are not of legal, moral, or ethical relevance and they are in line with research and education.

(1). Aristocratic use of ODINS – As an elite group in society, members of Osaka University should behave accordingly when using the Network. Materials of poor taste should not be communicated via ODINS.

(2). Awareness of other users – Transmission of large amount of data may affect other users of ODINS network. Therefore, adequate considerations should be taken into account when doing so. It should be noted that settings for checking email delivery with very short intervals can also impinge on co-users or even affect the operation of the network. Surfing web using a common facility of computer system and equipment for education such as Cybermedia Center should be kept to a minimum. When doing so, the interest of other users should be kept in mind.

(3). Proper maintenance of codes/passwords – codes and passwords are issued for the identification of authorized users. Therefore, they should not be passed onto friends, nor should they be allowed to use the facility via these codes and passwords. Both releasing and receiving codes and passwords will take responsibility for the possible consequences. The compositions of code and password should be considered carefully. Once determined, they should not be written down and they should be changed frequently. It should be intentionally avoided to observe others inputting their codes and passwords. Although no direct economic loss for many cases of stolen code/password, the authorized users may be considered responsible for any inappropriate activities occurred on the accounts. If accounts are used to hack into other computers, the authorized users are the primary suspects for the offence.

(4). Protection of privacy – In order not to allow other users access documents saved in common storage, access authorization is issued and it should be set appropriately. It is obviously very undesirable if anyone can access and/or modify secured documents. Conversely, accessing without authorization intentionally should be discouraged strongly. It is highly risky to post personal information on webpages or on display in network.

(5). Contribution to ODINS safety – Besides the above issues (1) to (4), to keep ODINS as safe as possible, authorized users should take precaution for their own activities as well. For example, introduction of virus should be always kept in mind. Suspicious emails should not be opened. Anti-virus softwares should be installed in the terminal computers of users' responsibility, and the softwares should be kept up-to-date. Any problems and malfunctions of ODINS should be reported to the system administrators immediately.

(6). Observation of netiquette – Other issues for network well being have been termed netiquette. Please refer the relevant web pages for more information (e.g. http://www.cgh.ed.jp/netiquette/)

5 Acknowledgement

This guideline is established with the reference of "User Guideline for Osaka Daigaku Information Network System".