

A Study on the Methodology of Information Ethics Education in Youth

Hoesung Ki *,

Sungkyunkwan University, Department of
Computer Education Ed.D. Student.

Seongjin Ahn **

Sungkyunkwan University, Department of
Computer Education Prof

Summary

In modern society the amount of daily information has been continuously and rapidly increasing with various new and improved mechanisms for finding, collecting and producing information. A problem with this trend is that it does not necessarily mean the improvement in information quality. A more serious problem is the unethical use of communications.

It is expected in communication, to have positive attitudes such as basic ethics, information ethics, communication etiquette, and the proper use of cyber language. We believe these positive attitudes can be achieved through school education programs. The current school program, however, seems inadequate and inefficient in providing these important elements of education to teenagers. Particularly in middle or high school for grades 7 to 12, it is crucial to develop and organize class materials for information ethics in order for the students to be aware of potential communication problems over the Internet. The effect of this education program will be not only to encourage the youth to have positive attitudes but also prevent them from having negative attitudes in daily Internet use.

In this study, we first review the current curriculum for the information ethics education, with respect to the contents and methodologies. We then analyze potential social or economic problems caused by the lack of communication ethics. As a result, we propose practical and effective education plans for information ethics education, based on current school conditions.

Key words: Information Ethics, Internet Ethics,

Computer Ethics, Cyber Ethics, students, Internet,

1. Introduction

The twenty first century can be defined as the emergence of the information age. Human society has evolved by passing through distinct stages, the first agricultural age, then, the industrial age, and finally, the information age. The Ministry of Education and Human Resource Development of Korea set a curriculum for computer-related subjects from the sixth curriculum, which was needed to reduce information illiteracy during this important transition. However, when understanding computers is considered as a cognitive sphere, the ability to use computer is considered as functional sphere, and the attitude towards computers is considered as sentimental sphere; this is true that an improvement in study materials has not been effective because emphasis has been put only on functional sphere of computers. Therefore, problems relating to the dysfunctional use of information have been raised as important issues in this society. These have included issues such as an internet-based crime, hacking, computer viruses, the collection of personal information, circulating unwholesome information, and the digital divide. In cyberspace, most people discuss issues they would not discuss in an actual physical environment.

This work was supported by grant No. (R01-2004-000-10618-0) from the Basic Research Program of the Korea Science & Engineering Foundation

They feel more comfortable, less restrained, and want to open themselves up. This phenomenon is called the disinhibition effect (Suler, 2002). Individuals generally share very personal matters such as their feelings, hopes, and fears with others in cyberspace. However, this disinhibition effect is not always beneficial to society. Individuals also use offensive language, apply severe criticism, hatred, and menace, or even associate with lascivious or violent websites.

Considering the above, interacting in cyberspace requires a higher standard of morality than that required in a physical world. Finally, information ethics should be added to the curriculum for youth, in order to help them develop good manners, and exist as constructive members of a modern information society.

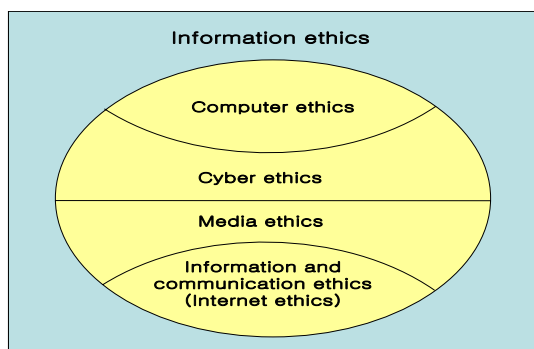
This study proposes methods to put positive functions of information to proper use, particularly, laying emphasis on making information ethics a chapter of computer education, and discussing the contents a chapter should contain, with a method of education emphasizing not only the dysfunctions but also the positive functions of information.

2. Theoretical Contemplation on Information Education

2.1. Concept and Characteristics of Information Ethics

Information ethics has been developed since the 1980s, encompassing areas such as computer ethics and global information ethics.

The terms that are used when describing information ethics in books or over the Internet are defined in [Fig 1].



[Fig 1] Similar terms

- Computer ethics is a standard for computer use, signifying the prevention of copyright infringement, such as the reproduction of software, invasion of privacy, and circulation of objectionable material.
- Cyber Ethics is a system of standards that prescribe morality and immorality in cyberspace, signifying the preservation of freedom of expression, intellectual property, and privacy.
- Information and communication ethics is a system that solves ethical problems caused in an information society, defined under the term, Internet ethics.
- Media ethics signifies that media restricts and regulates the antisocial and immoral aspects, obstructing the formation of a social personality.
- Information ethics relates to questions of ethics in terms of information or an information-oriented society. This includes the standard for judging behavior of an individual or a member of community and classifying these as moral or immoral.

All in all, as far as we are concerned that “information ethics” implies all the similar terms above, it is most suitable to use the term, “information ethics” in order to understand the concept.

When analyzing the characteristics of information ethics, we can see that even though ethics has been emphasized absolutely and universally, it has actually occurred as a function of local ethics. In conclusion, information ethics in the future should be a discipline that carries out functions as shown in [Fig 2].

First, information ethics is prescriptive ethics. It must clearly prescribe what to do and what not to do in information society.

Second, information ethics is preventive ethics. It must help us give careful consideration on all types of ethical problems the development of information and communications technology produces.

Third, information ethics is transformative ethics. It must put emphasis on the necessity of human experience and the transformation of the system and policy. This is because it appears as a reaction against the dysfunction of large amounts of information, especially, the disorder and chaos in cyberspace.

Fourth, information ethics must be universally global ethics, not one or the other, but must consist of both global and local disciplines.

Fifth, information ethics is responsibility ethics. It must promote behavior as a sense of responsibility, considering the possibility of an action according to the view of a means and a method, while comparing a purpose to incidental results.

Sixth, information ethics is comprehensive ethics. It must synthesize and utilize various ethical theories that are useful in solving ethical problems in both direct and indirect ways.

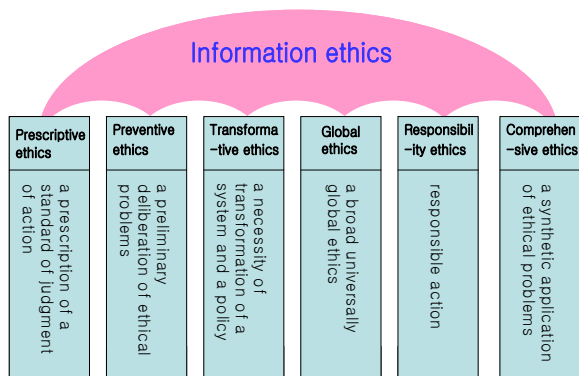


Fig 2] the characteristics of information ethics

2.2 Goals and Basic Principles of Information Ethics

For the proper use of information in an information society, the education relating to information ethics may present its goals as follows:

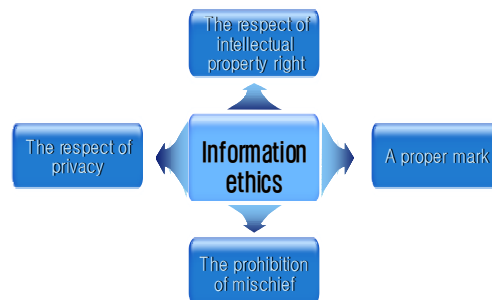
- First, respect for others must be cultivated.
- Second, although sharing beneficial information is welcome, other people's intellectual property right must not be infringed.
- Third, various forms of information will be used productively.
- Fourth, telecommunications and the Internet will be used for acceptable time periods so that it does not harm actual life.

Richard Severson presented four basic principles of information ethics, as the respect of intellectual property rights, the respect for privacy, a proper mark, and the prohibition of mischief. These are shown in [Fig 3].

- First, the respect for intellectual property, which stands on the basis of a cultural conviction that original work remains the property of its owner.
- Second, the respect of privacy, which we have to deal with actively with more specific information.

Third, a proper mark, which is related to how sellers inform customers about their goods and services. This is when ethics teaches us the ethical root of the rule of responsibility.

Fourth, the prohibition of mischief, which means to refrain from damaging other people, directly or indirectly. This guides us to improve our ethics when computer crime or hacking is involved.



[Fig 3] basic principles of information ethics

3. The Actual Condition of a Dysfunction of Information Use

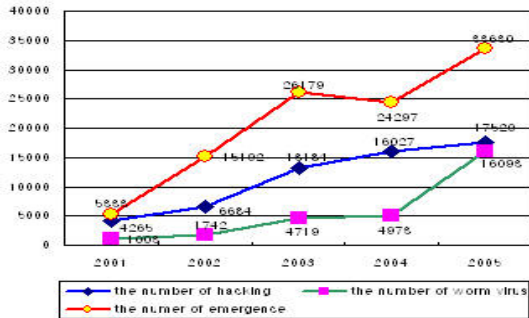
Internet crime, otherwise known as cybercrime, has involved intelligent, automated, larger-scale, distributed attacks, causing serious damage.

In the past, hacking primarily displayed the hacker's ability, however, modern hacking has evolved into antisocial actions, using the hacker's knowledge for a criminal intent. Looking into the subject of hacking according to various situations, hackers have no regard for selling, distributing, falsifying, or destroying confidential information of a country, company, or individual.

This is regarded as a result of a lack of proper information ethics, which is in turn, caused by the perception of being anonymous in cyberspace. It is found that Korea's hacking-related occurrences have grown considerably in the last five years as shown in [Fig 4]. This is not a local problem, and the whole world needs to teach the youth to understand the rules and ethical spirit, to be respected even in cyberspace.

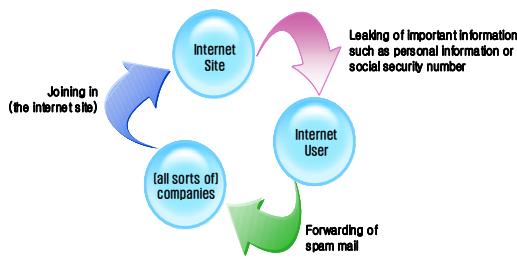
According to the changes in the information society, it is common for personal injuries of revelation and forgery by malicious individuals obtaining databases with personal information, penetrating weak security systems. The most common reported disclosure of

personal information is defamation of personal information, and ID theft. This most often arises from



[Fig 4] the present condition of reported hacking, worm, and emergence

damage caused by stealing social security numbers. Enumerating reported invasions of personal information in order of frequency, we obtain the following invasions of personal information, the receipt of unwanted information, the refusal of correction of personal information or membership succession, collecting or distribution personal information without the individual's agreement, transferring information, and the disregard to safety when collecting information. Considering the types of an invasion of personal information, the channel of invasion is shown in [Fig 5].



[Fig 5] Types of invasion of personal information

The other point at issue is that the flowing of objectionable information in cyberspace is spreading in relation to the increase of users and connected computers. The types of objectionable information and volume are both increasing. The types of objectionable information include the following, pornography, violent movies, invasion of intellectual property right, cyber sex, cyber gambling, stalking, and unlawful marketing.

4. Contents of Information Ethics

Education

4.1 Communication Etiquette in Cyberspace

Cyber rights include the freedom of expression, and cyber duty is the obligation not to injure others in an information society. The subsequent sections explain the basic idea of ethics such as responsibility, ownership, privacy, and the respect of others.

First, cases of insulting and disrespecting others are increasing. For this reason, the fundamental rules of manners and netiquette in communications should be established, basic etiquette of using the Internet should also be taught.

[The fundamental rules of netiquette]

- † Internet users should respect themselves and other Internet users.
- † Internet users should understand that data and articles contain the user's personality when the user submits the information over the Internet.
- † Internet users should not enforce their opinion but listen to other's opinions when they discuss a topic.
- † Internet users should try to share wholesome and beneficial information.
- † Internet users should try to set a time limit for discussion, and finish it within restricted time, when they chat or debate an issue on the Internet.

Second, netizens usually use abbreviations or slang as a way to speak their mind. In particular, as a result of using mobile communications as well as Internet, teenagers tend to use phonetic words, and orthographical rules are being ignored. Consequently, education of the proper use of language, by providing telecommunication language rules is needed.

[The fundamental rules of using telecommunication language]

- † No vulgar language is allowed on an Internet chatting space or boards.
- † No abuse, insulting, or gossip in cyberspace.
- † Abbreviations or slang should be restricted as possible.
- † No phonetic words are allowed, and orthographic words should be used instead.
- † Internet users should use proper language in good manners comparable to a face-to-face situation.

Third, it is usual to use the Internet for longer hours than expected. This happens more to teenagers

because they have less control over themselves, when the use of telecommunication should not hinder everyday life. Therefore, addiction should be determined from the use of an Internet addiction test, and if any addition is found, this should be gradually remedied. Also, it is required to issue guidelines for Internet usage.

[Guidelines for Internet use]

- † Internet users should observe the proprieties for communicating over the Internet.
- † Personal information such as name, address, social security number, or contact number should not be exposed.
- † Internet users should inform their instructors when they receive a solicitation from others over Internet.
- † Intellectual property rights relating to information obtained over the Internet should be protected.
- † Internet users should not connect to sites, which include violence, rumors, or pornography.
- † Internet users should not link to undesirable sites, for example, a community of suicidal fanatics.

- † Internet users should try to connect to sites that include sound and desirable contents.
- † Internet users should not install software on school computers for the purpose of personal use. In addition, illegal software cannot be used.
- † Internet users should try to use Internet as long as planned.
- † Internet users can ask any questions to their instructors.

4.2 Information Security and Ethics-related Laws

It should be understood by the youth that hacking is a criminal offence, hurting other people. Methods for protecting an individual’s computer system should be taught. Accordingly, the fact that spreading viruses damages other people and the prevention of virus attacks should be taught, the youth should protect their system by learning about precautionary measures against viruses as shown as [Table 1].

[Table 1] Computer Information Security

Provision against Hacking	<ul style="list-style-type: none"> • Properly qualified users could be allowed to connect to the network, and “guest” accounts should be as restricted as possible. • Network administrators should always use up-to-date software, especially, updating to the latest anti-virus program in order to prepare for any potential viruses. • For the provision against loss of information, data should be backed up periodically according to a fixed backup schedule. • Unlawful scanning of important information committed by external connectors must be reported. • Thorough technical security is more important than the simple disconnection of a hacked computer.
Provision against Virus	<ul style="list-style-type: none"> • Always install the latest version of an anti-virus program, and update it at least once a week. • Set up a program to automatically scan the computer for viruses once a day. • Check for viruses before every file download or upload. • Use system surveillance to prevent an infected file from running. • Use legitimate software, not illegal software. • Back up any important files. • Approve sharing network files only under a state of safety. • Do not connect to any sites that are known to be frequently infected by viruses.

The possible types of information crime that the youth could commit on the Internet include violating intellectual property rights. Intellectual property rights involve intellectual property creation, including trademark protection, patent rights, and copyright.

Therefore, teenagers who do not understand the legal protection of intellectual property rights might not understand the implications, and may think they are just doing what other people are doing. Consequently, information ethics education should thoroughly explain

Laws	Contents
Constitutional Law	Clause 21, Art. 4: The press and the publication shall not discredit others or infringe the rights of others, public morality, or social ethics. If the press or the publication hurt the dignity or rights of others, the sufferer can claim compensation.
The Telecommunications Business Act	Clause 53, Art. 1, No. 1: The Prohibition of Illegal Communication. Clause 53, Art. 2: (The Regulation of Unhealthy Communication) The subject of communications threatening public peace and order, or good and beautiful custom is stipulated by the Presidential decree.
The Digital Network Act	Clause 50 Art. 1: the Restriction of forwarding commercial contents. Clause 50 Art. 3: The Restriction of commercial voice information. Clause 50 Art. 6: The restriction of commercial forwarding by automatic creation of the receiver's connecting location. Clause 42 Art. 2: the restriction of forwarding commercials for hazardous articles to the youth, and so forth.
The Decree on expansion of telecommunication network and promotion	Clause 25: (Protection of Secret and the like) No one is allowed to injure, infringe, steal, or reveal information, handled, kept, or transmitted by telecommunications networks. Clause 61: Defamation, Clause 62, No. 1: conveyance or spread of virus or virulent programs, Clause 62 No. 5: service refusal assaults, Clause 63 No. 1: expansion of the penalty on protection conducting violation to digital network violations, Clause 65 Art. 1, No. 2: Filthy Communication, Clause 65 Art. 1 No. 3: Cyber stalking, and so forth.
The younger generation Protection Act	Clause 10: (deliberation standard for media of detrimental against the youth) 1. Anything lascivious or lewd, which stir up sexual desire of the youth. 2. Anything that might inspire violence or crimes in youth. 3. Anything that incites the youth to, or embellishes drug abuse or violent action including sexual assault. 4. Anything antisocial or unethical that obstructs the formation of civil awareness and healthy personality of the youth.
Criminal Law	Clause 243: (the distribution of negative prints) Those who distribute lascivious documents, books, films, or the like may put in jail for up to one year, or be fined up to 5,000,000 won. Clause 244: the production of negative prints, Clause 245: pornographic performances, Clause 307: defamation, and so forth.
The Decree on the punishment for sexual assault and protection of victims	Clause 14: (Lechery of communication media use) Those who give words, sounds, writings, books, images, or objects to others through telephone, postal service, computer, or any other communication media with the purpose of inducing sexual desire of themselves or others may be put in jail for up to one year, or be fined up to 3,000,000 won.
Additional	<ul style="list-style-type: none"> •The organic law for the promotion of information. •The Act for Telecommunication Secrecy •The act for information and communication foundation protection •The Decree on public institutions and personal information •The act for the protection of computer program •The Copyright Act, The Patent Law, The Design Right Act

[Table 2] Laws on penalty against unhealthy information and communication

related laws. Particularly, unlawful copying of software, as this is widespread, and shows us the importance of explaining that it is committing theft and violating people's intellectual property rights. In addition,

websites require attention, such as those that relate to suicide, linguistic violence, insulting, hacking, the

5. The Methodology of Information Ethics Education

5.1 The Method of Education

The method of educating information ethics is to be presented in five models, an illustrating model, researching model, example model, activity model, and case study model. The difference between the proposed methodology and the current system includes the following. The attention to the actual experience in cyberspace, scanning the aspect of legal punishment and informational ethics comprehensively, indirect experience through case study, and the establishment of correct values for actual and practical use in an information society.

First of all, in an 'illustrating model', instructors should correctly illustrate basic ethical concepts to the youth in order to help them understand characteristics of ethics in an information society. Instructors should weigh semantics, distinctiveness, versatility, interest, conciseness, concreteness, logical order, and inclusiveness to explain the characteristics clearly.

Second, in a 'researching model', instructors should not only offer the youth possible subjects, which they can search for, but also let the youth make the ultimate choice. Instructors can make the youth study additional diverse subjects such as internet and PC communication etiquette, information-and-communication-ethics-related law, the influence of violent information and lascivious information, the influence of hacking and spread of virus, the importance of privacy, the importance of copyright, and internet real name policy.

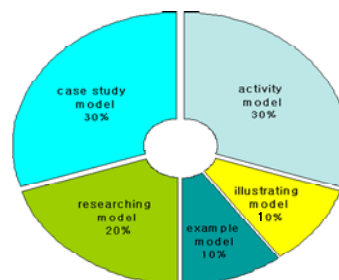
Third, in an 'example model', instructors should use various devices such as films, slides, video tapes, articles, or comics related to the study of information ethics. For example, when an instructor teaches netiquette, the instructor will show the students data retrieved from an insulting community or swearing community, and let the students understand the seriousness of insulting and swearing; this gives the

distribution of pornography, forgery or alteration, and invasion of privacy. Information ethics-related laws against unhealthy information and communication are shown as [Table 2]

students an opportunity to realize the gravity of internet addiction themselves.

Fourth, in an 'activity model', instructors should provide the youth the chance to experience diverse activities to develop their speculative ability. For example, pasting newspaper clippings into a scrapbook and analyzing the problem, reviewing unhealthy information for teenagers on the Internet, or role-playing situations relating to netiquette.

Fifth, in a 'case study model', instructors lead the class concentrating on real cases initiated by the students. For example, those who hurt others by writing distorted facts or rumors, or exaggerating certain facts would not be punished by law, but be punished by school policy. Students can discuss how to behave in real life after having an indirect experience through case studies.



[Fig 6] education method application rate

Reviewing the methods above, the illustrating model and example model focus on instructors, and researching model and activity models focus on the youth. Recently, educational methods have evolved from instructor-based methods to learner-based methods, laying emphasis on actual experience and stimulation of self-led learning.

In conclusion, the percentage of illustrating models and example models should be decreased, and the percentage of researching, activity, and case study models should be increased as shown in [Fig 6]. In addition, the methods mentioned above are related to the ICT(Information & Communication Technology)

utilization class which is accentuated by the Ministry of Education and Human Resource Department. Namely, it has been changed in information societies from linear, graduated, and uniform education to hypermedia education, from cramming education to participating and constituting education, and from notifying teacher to promoting teacher.

Therefore, using advanced teaching devices, such as the Internet, powerpoint presentations, and various homepages will contribute to the efficiency and effectiveness of education. This requires the effective class arrangement and teacher’s thorough preparation for the class. Accordingly, it is required to sets up practical rules, and practices through discussions based on case studies.

5.2 Application Plan

Education contents presented in chapter 4 can be exhibited as shown in <Table 3> applying methods of education. The order of application is shown in Roman letters below.

<Table 3> Application of information education contents and education method

The contents of education The education method	Human obligations and rights in cyberspace	Telecomm-unication etiquette	Using telecommu-nication language	A method of prevention against telecommuni-cation addiction	The intellectual property right and software	Computer security and a method of prevention against virus	Information ethics-related law
Illustrating model	I				I		I
Researching model		I		I	II	I	
Example model	II		I				
Activity model		II	II	II		II	II
Case study model		III		III	III	III	III

First, results will be achieved by applying the ‘illustrating model and the ‘example model’ for human obligations and rights in cyberspace. The ‘illustrating model’, explains everything relating to the basic concept of ethics. The ‘example model’, provides the youth with related material such as press news or comics, to show the effectiveness of following human obligations and rights in cyberspace.

Second, for telecommunications etiquette, will be useful applying the ‘researching model’, the ‘activity model’, and the ‘case study model’. The ‘researching model’ allows the youth to chat online and read the Internet board by themselves. The ‘activity model’ takes an oath of proper telecommunications language use. The ‘case study model’ involves searching for actual

examples of violations in cyberspace.

Third, applying the ‘example model’, and the ‘activity model’ will be necessary for using telecommunication language. The ‘example model’ uses related materials provided by instructors, and the ‘activity model’ pledges the youth to use proper telecommunications language.

Fourth, it will be effectual to apply the ‘researching model’, the ‘activity model’, and the ‘case study model’ for a method of prevention against telecommunication addiction. As a method of prevention against telecommunication addiction, the ‘researching model’ is used, for examining Internet addiction, the ‘activity model’ discusses telecommunication rules, and the ‘case study model’ studies practical influences on Internet addiction.

Fifth, for intellectual property rights of software, it will be effective to use the ‘illustrating model’, ‘researching model’, and the ‘case study model’. The ‘illustrating model’ gives an explanation for the concept of property rights. The ‘researching model’ lets the youth research the relations between intellectual property rights and software, and the ‘case study model’ illustrates examples of surreptitious use of intellectual property..

Sixth, for examples of virus problems and computer security, the application of the ‘researching model’, the ‘activity model’, and the ‘case study model’ will be useful. The ‘researching model’ gives an opportunity to look for the data related to security and viruses individually, the ‘activity model’ is used to decide the virus protection method, and the ‘case study model’ is used to search for material.

Seventh, using the ‘illustrating model’, ‘active model’, and the ‘case study model’ will be helpful for information-ethics-related laws. The ‘illustrating model’ gives an explanation regarding laws relating to information ethics, the ‘activity model’ is used to share teenagers’ different opinions, and the ‘case study model’ concentrates on information –ethics related crimes and punishments.

Consequently, the application of information ethics education can be shown in [Fig 7]. The curriculum for school education is detailed below.

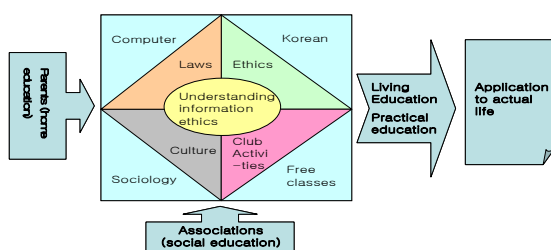
First, the first unit of the textbook for information society and computer class should be ‘understanding information ethics’, and the topics mentioned above

should be contained in this section. Related subjects, such as Ethics, Sociology, Korean, Technique and Housework, should lead to a debate concentrating on information ethics.

Second, arranging an independent curriculum for information ethics can be a good plan; however, this will be excluded according to the tendency of reduction and unification of a subject.

Third, classes related to information ethics should be provided in free classes or as club activities, and a test on information ethics should include a Korean listening test, essay writing test, and interview.

Parents should operate 'living education' through home education, related associations also should provide 'practical education' through a social education network.



[Fig 7] the range of application of information ethics education

6. Conclusion

To settle information and communication ethics systems, the schools' role regarding information and communication ethics education is more important than any other organizations' role. The regulation of law and the protection policy of the government is limited, and cannot fully provide the internet users spirit of responsibility and ethics. Therefore, education for growing youth should be furnished through proper information ethics education, school, home, and the society should try hard to promote social education in the entire educational environment. The socialization process should be flexible, repetitive, and provide interaction with others. Through this socialization process, youth who are participating in school education will establish their own autonomous responsibility and the spirit of ethics. This study started from the opinion that the sentimental sphere is more important than the other two spheres, the cognitive or functional sphere. As a consequence, a computer education course of information using dysfunctions of information use,

present conditions of information ethics education, 'understanding information ethics', and applying information ethics education are suggested. Accordingly, the ultimate question on the settlement of ethics education system is to try and foster Internet users who have the power to recognize and understand information ethics, and to create an ideal knowledge information society.

References

- [1] Information Communication Ethics Committee, KIPS, IT Certification(2004), Internet Ethics, I-Han
- [2] Yang, Min-Young and Park, Sun-Ju(2000), Curriculum of Information Communication Ethics Education Process Model Development for Elementary Schools, Korean Information Education Society Collection of Papers
- [3] Chu, Byoung-Wan(2001), An Essay on Information Ethics Education, Ullyouck Press
- [4] Seoul Metropolitan Office of Education(2001), How to Educate Cyber Ethics, Information and Communication Ethics Education for Secondary School Teachers
- [5] Song, Su-Kum(2002), Study on the contents of Information Ethics Education and the Methodology of Education for Secondary Schools, SungKyunKwan University Press
- [6] Brey, Philip(2000), "Disclosive Computer Ethics," Computers and Society, Vol. 30, No. 4, December, pp. 10-16. Reprinted in R. A. Spinello and H. T. Tavani, eds., (2001). Readings in Cyber Ethics, Sudbury., MA: Jones and Bartlett Publishers.
- [7] Floridi, Luciano(1999), Information Ethics: On the Philosophical Foundations of Computer Ethics, Ethics and Information Technology Vol.1, No.1, pp.37-56.
- [8] Richard Severson(2000), Translated by Chu, Byoung-Wan and Ryu, Ji-Han, Fundamentals of Information Ethics, Philosophy and Reality
- [9] Lee, Kyoung-Wha(2003), Efforts for the Fixation of Systemic Information and Communication Ethics Education, Information Communication Ethics Committee

- [10] Sylvia Clark Pulliam(1994), Ethics and Computer Scientists, National Educational Computing Conference.
- [11] Janine DeWitt-Heffner(2001), Carolyn Oxenford Marymount University, Defining the Limits: Cyber Ethics.
- [12] Nancy Willard(1997), Moral Development in the Information Age, Proceedings of the Families, Technology, and Education Conference(chicago, IL, October 30-November 1, 1997);see PS 027 175.
- [13] Stanford Encyclopedia of Philosophy(2001), Computer Ethics: Basic Concepts and Historical Overview.
- [14] Bynum, Terrell Ward(1999), The Foundation of Computer Ethics, a keynote address at the AICEC99 Conference, Melbourne, Australia, July 1999. Published in the June 2000 issue of Computers and Society.
- [15] Byunm, t. w., & Rogerson, s.(1996). Global Information Ethics, Science and Engineering Ethics. 2(2).
- [16] Tavani, Herman T. and James H. Moor(2001) " Privacy Protection, Control of Information, and Privacy-Enhancing Technologies", Computers and Society Vol.31, No.1, 6-11.
- [17] Nissenbaum Helen(1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public, W: "Law and Philosophy", Vol.17, s559-596.
- [18] Hoven, J. V. D.(2000), The Internet and varieties of moral wrongdoing, In D. Langford, Internet ethics, New York: St. Martin Press.
- [19] Gotterbarn Donald(2001), Informatics and professional Responsibility. W: Science Engineering Ethics; Vol.7, nr2.
- [20] Johnson Deborah G.(2001) Computer Ethics in the 21st Century. Referat Plenarny na konfer ETHICOMP '99, Rzym, październik 1999. W: R. A. Spinello, H. T. Tavani(red.), Reading CyberEthics. Jones and Bartlett.
- [21] Ermann, M. David(1997), Computer ethics : cautionary Tales and ethical dilemmas in computing, Oxford University.
- [22] David Berryand and 19 more authors(2000), Ethics and Media Culture, Focal Press.
- [23] Richard A, Spinello & Herman T, Tavani,(2002) Readings in CyberEthics, Second Edition.
- [24] Computer Ethics Bibliography, by Herman Tavani (Rivier College)
- [25] National Computerization Agency(2005), Korean Internet White Paper
- [26] Ministry of Information and Communication(2005), Information Protection in the Age of Internet
- [27] <http://www.icec.or.kr>
- [28] <http://www.krcert.org>



Hoesung Ki received the Konkuk University Computer Engineering M.S, and Ph. D. Candidate in department of computer education from Sungkyunkwan University, Seoul, Korea, in 1994, and 2006, respectively. I was a

researcher in KIST/SERI, Daejon, Korea. I am currently staff in the Sungshin Woman University Office of Information and Communication. My research interest include Internet management, network security, Computer Engineering, Computer education and Internet ethics.



Seongjin Ahn received the B.S., M.S., and Ph. D. degrees in information and communication engineering from Sungkyunkwan University, Suwon, Korea, in 1988, 1990, and 1998, respectively. For more than five years, he was a researcher in

KIST/SERI, Daejon, Korea. He is currently an associate professor in the department of computer education, Sungkyunkwan University, Seoul, Korea. His research interests include Internet management, network security, and Internet ethics.