e-GUARDIAN Version 2.0 Syllabus

Category	Ref.	Task Item
1. Basic knowledge on e-safety	1.1.	Understand the differences of information contents (open, private, business, etc.).
	1.2.	Be aware of privacy protection legal act (be aware of the responsibility for own actions on the Internet: do not publish the information without permission, be responsible by writing comments, do not download music, movies, etc.).
	1.3.	Know about equity between opportunities & risks of web2.
	1.4.	Understand the notion of identity.
	1.5.	Be aware of different identity for authorization theft methods (skimming, pretexting, shoulder surfing, information diving).
	1.6.	Know about social engineering and it's methods.
	1.7.	Be aware of cyber crime, online predators, financial scams, harm and who to contact if discovered illegal data.
	1.8.	Understand computer infection threats (viruses, Trojan horses, spyware, dishonest adware, etc.). Know when and how malicious software can get into computer system.
	1.9.	Know about organizational security: school security, usage of school web pages, content publishing, access, etc.
	1.10.	Know about netiquette and other basic codes of conducts in the cyberspace (RFC 1855).
	1.11.	Understand what is Online Safety 3.0 and why digital citizenship is protective.
2. Privacy and data management	2.1	Distinguish between data and information.
	2.2	Understand the opportunities and risks of digital data management from fully collaborative to full privacy.
	2.3	Know about multi-layer password, changing and keeping password policies.
	2.4	Know about safe computer login methods.
	2.5	Know multiple user accounts on various digital environments. Understand the meaning and importance of access rights (what a personal user account is and how data of different users is separated).
	2.6	Be aware of data encryption, decryption and password protected files.
	2.7	Understand what intellectual property on Internet is.
	2.8	Understand the benefits and purpose of data backups and be able to restore lost data.

Category	Ref.	Task Item
3. Security tools and network security	3.1.	Know computer network types (local area network (LAN), wide area network (WAN), virtual private network (VPN)) and why protection is needed.
	3.2.	Know different network connection methods (Cable, Wireless, Mobile networks).
	3.3.	Be able to use wireless network safe and know how to connect to a protected/unprotected wireless network.
	3.4.	Sharing and accessing resources over network (Files, Printer, Desktop).
	3.5.	Understand safety means of computer networks (Firewall, Antivirus, Anti-spyware, Spam blocker Password protection, Connection encryption – wireless).
	3.6.	Be able to use standard OS integrated protection tools.
	3.7.	Be able to turn on / off and adjust protection level in standard security means that are integrated in the operating system (Firewall, Protection tools, etc.). Distinguish different modes of antivirus protection (active, passive).
	3.8.	Know what has to be done and in what order, if you suspect that computer system is infected. Distinguish infected files deletion, quarantining and curing.
	3.9.	Know how to follow, download and use updates for your operating system, software and importance of antivirus definition files. Understand the benefits of these updates.
	3.10.	Informal and formal periodic external checkup.
4. Minors and newcomers on the net	4.1	Understand the impact of communication with minors and new users about safety in IT World.
	4.2	Understand the purpose of monitoring, filtering and controlling tools for safer internet use of minors.
	4.3	Be aware of different ways to educate, monitor and control usage of social networking and other web sites.
	4.4	Be able to develop policies and apply methods for children's use of the computer and the Internet (depending on age and socio-cultural situation).
	4.5	Understanding advantages and limitations with protection software.

Category	Ref.	Task Item
5. Social networks and safe usage of the Internet	5.1	Know how to start and finish safe browsing session (https, lock icon, always logout and close the browser window). Know consequences of unsafe browsing.
	5.2	Know about advantages, disadvantages and dangers of Internet cookies and ActiveX control. Know about tools that ensure safety when browsing the Internet.
	5.3	Be able to manage: temporary Internet files, browser history, passwords, cookies and autocomplete data.
	5.4	Be able to safely connect to e-Services and secure environments– connecting and using, recover lost passwords.
	5.5	Know when and in which cases personal information can be published on the Internet (i.e. status publishing about leaving home).
	5.6	Know who you should contact if you discovered inappropriate information about you or your related digital identities.
	5.7	Understand that it is necessary to exercise critical thinking about content and identities on the internet. (i.e. blogs, Wikipedia, social networks, forums, etc.).
	5.8	Understand 'threats of inappropriate content for different groups of people (duality of personality, psychological harm, racism, religious sect, alluring to buy something or disclose your information, information about drugs, violence and so on).
	5.9	Understand what an online social network is, what are opportunities and risks of social network. Age groups of using social networks. Options and parameters for information disclosure. Understand what is the fascination to disclose private information on the internet.
	5.10	Know different social network types (Friendship-driven and Interest-driven) and be able to use them harmless and safe (appropriate account privacy settings).
	5.11	Know what type of information recommended to be published on social network, be responsible for published content, and know impacts.
	5.12	Understand that online socializing reflects "real life".
	5.13	Be able to send/receive e-mail securely: know how to reject email from specific email addresses. Know how to treat email messages from unknown senders, classified as spam and email messages infected with malware. Know about scam, hoax, chain letters.
	5.14	Be aware of safe instant messaging. Understand confidentiality while using IM like: file sharing, non-disclosure of important information, etc.
	5.15	Understand threats of online communication: virtual dating, bullying, commenting.
	5.16	Understand dependency and addiction to the Internet.