IMT SCHOOL FOR ADVANCED STUDIES LUCCA

REGULATIONS TO USE THE INTERNET AND E-MAILS

Chapter 1 General Characteristics

Article 1 - References

1. These regulations are a formality, provided by the provision of the Privacy Guarantor published in the Official Gazette no. 58 of 10 March 2007. This provision requires public and private employers to draw up a specification concerning the use of the internet and e-mails in workplaces, indicating to what extent and in what manner checks are carried out.
2. These regulations have been drafted by considering the references to the policy of use of the internet by GARR (research network allowing connection to the Internet), the Google Apps for Education contract, the privacy policy of Google and Netiquette.

Article 2 - Purpose and scope of application

1. These regulations establish the conditions of use of e-mails, network connectivity and information systems provided by the School, to support teaching, research, administration and other activities related to the School's institutional purposes. The service offered to the user is subject to the acknowledgment of these regulations in all parts and to the complete acceptance without reservation of the foreseen conditions.
2. The user identifies him/herself to e-mails, network and information systems through distinct credentials. Credentials are pairs of usernames and passwords; access to e-mails can be strengthened by a two-step verification.
3. All the School's telematic services are managed by the Infrastructures, IT services and digital administration office, which also identifies the system administrators for the various services.
4. Users who are entitled to the credentials to access the various services and the duration of these credentials are defined by a specific regulation or general provision of the School.

Chapter 2 E-mails

Article 3 - Google Apps for Education

1. The School's e-mail service is part of the services called Google Apps for Education and is provided by Google Inc. ("Google"), located at1600 Amphitheatre Parkway, Mountain View, CA 94043, United States, according to the terms of the Google Apps for Education Agreement.
2. The credentials to access e-mail services provided by the School allow access to its institutional mailbox.
3. Anyone who uses a school mailbox is informed that IMT administrators are provided by Google with the technical means to access, monitor, use account data and accept:
   a. that your data can be stored in *datacentres* outside Italian borders;
   b. Google's terms of service and privacy policies that must be accepted the first time you access your mailbox;
   c. the service levels defined in the Google Apps Service Level Agreement (SLA) document.

4. The user of the mailbox undertakes to:
   a. not generate or facilitate collective e-mail messages not required for commercial purposes;
   b. not violate or encourage the violation of others' rights;
   c. not pursue any unlawful purpose of intrusion, violation, defamation or fraud;
   d. not intentionally spread viruses, worms, Trojan horses, damaged files, hoaxes or any material of a destructive or deceptive nature;
   e. not send or memorize messages of an outrageous and/or discriminatory nature by sex, language, religion, race, ethnic origin, opinion and union and/or political affiliation;
   f. actively seek to safeguard the confidentiality of your password and to report any situation that could affect it
   g. comply with the provisions of Article 11 of the IMT Code of Conduct

   The list is not intended to be exhaustive.

Article 4 - Institutional mailbox

1. A credential is created for each eligible user to access the institutional mailbox, whose username is in the name.surname@imtlucca.it and a short *alias*, firstletterofname.surname@imtlucca.it (some previous accounts could be set differently, that is, the main credential in the form of firstletterofname.surname@imtlucca.it and an alias in the name.surname@imtlucca.it form).
2. The *alumni* or former students of the School maintain their mailbox through the aliases, but the main username is transformed into the name.surname@alumni.imtlucca.it form.
3. The activation and deactivation of the institutional mailboxes is the responsibility of the system administrators. For justifiable reasons, it is possible to request the forwarding of your mailbox to a personal mailbox even after the deactivation or expiry of the terms.
4. Access to an institutional mailbox by multiple users at the same time is not permitted.
5. The School equates e-mails between internal users to open paper correspondence; the user states to be aware that internal correspondence can be viewed by the employer.

Article 5 - Access without assent

1. The School does not inspect or access the user's e-mail messages without their authorization. The School can allow or arrange the inspection, monitoring or access to the users' e-mails, even without the consent of the holder, in the following cases:
   a. upon written request of judicial authorities in the cases foreseen by current legislation;
   b. upon notifying the user, for serious and proven reasons that lead to the belief that the current legal provisions or rules defined in the following regulations have been violated;
   c. in critical and emergency situations.
2. The School may allow the user password to be reset if it is reasonably deemed that the credentials have been stolen without the user's knowledge

Article 6 - Security and confidentiality

1. E-mail messages may be subject to automatic inspection both by Google (see Google's privacy policy) and anti-virus and anti-spam software.
2. The fundamental objective of the School is that e-mails are safe and reliable, even by promptly interacting with Google technical support. It should however be reminded that the security and confidentiality of e-mails cannot be guaranteed in all circumstances, especially regarding e-mail messages downloaded onto personal devices. In this case, it is essential that the user implements the appropriate actions to protect information by using all available means.

Article 7 - Distribution lists

1. With the provision of the School, the distribution lists of all the School staff are defined and divided into categories and functions. Subscription to the distribution lists is automatic once the institutional mailbox has been assigned.
2. The distribution lists are used for the dissemination of information of general interest and however, of service to members.

Article 8 - Distribution lists, unsolicited messages

1. Automatically classified messages (from the antispam filter and anti-virus software) as unsolicited and addressed to the distribution lists are placed in a moderation queue, waiting to be completely eliminated.
2. Users must keep in mind that in fulfilling their duties, the system administrators may display a message addressed to a distribution list erroneously marked as spam. However, such staff is however required to comply with strict confidentiality restraints if the aforementioned cases should occur.
3. To limit the number of unsolicited messages, the system administrators choose, depending on the use of the distribution list, to restrict the list of possible senders by using the different options available; for example, it is possible to give the right to send e-mail messages to a specific distribution list only to those who are part of it.

Article 9 - General e-mail addresses

1. In the transparency page, the general e-mail addresses managed by the offices are published in the section relating to the organization of the offices.
2. It is possible that a given office will be associated with more general e-mail addresses to better allow the sorting of e-mails divided by office activities.
3. The general e-mail addresses are managed by using the technique of the distribution lists and are, by all means, to be considered distribution lists. Unlike ordinary distribution lists, general e-mail addresses are allowed to send e-mail messages with e-mail sender addresses of the distribution list. When an email is sent with the aforementioned methods, a copy of the message is automatically delivered to all members who are part of the distribution list that defines the general email address. This establishes the collaboration of the activity among all the members of the distribution list.
4. Thanks to the mechanism of the distribution lists, it is possible, without operating directly on the individual workstations, to enable or disable access to general e-mail addresses by acting directly on the server administration panel. System administrators can indeed make immediate changes to the members of the distribution list (and therefore, of the general e-mail addresses) from the administration console, at each change to the organization of offices or activities.

5. Exceptionally, if a single person has access to a general e-mail address, the address can be managed via a traditional mailbox, which is the responsibility of the person who accesses it. In these cases, access to the general mailbox is not foreseen if the holder is absent from work.

Article 10 - Certified e-mail address (PEC)

1. The certified e-mail address of the School, imtlucca@postecert.it, is assigned to the office responsible for sorting incoming certified mail. Sorting and registering take place through the interface of the IT protocol management software.

Chapter 3 Access to the School's Internet

Article 11 - Access to the Internet

1. Access to the School's Internet is provided by GARR though the research network.
2. Each user of the Internet service accepts the rules of access to the internet reported in the document called GARR Acceptable Use Policy - AUP.
3. The following activities are not permitted on the internet:
   a. providing parties that are unauthorized to access the internet with the service of network connectivity or other services included in it, such as the provision of housing, hosting and similar services, as well as allowing the transit of data and/or information on the GARR network between two parties, which are both unauthorized to access the internet (third party routing);
   b. spread viruses, hoaxes or other programs in a way that damages, harasses or disturbs the activities of other people, users or services available on the internet and those connected to it;
   c. create or transmit or store (if not for research purposes or in a truly controlled and legal mode) any image, data or other material that is offensive, defamatory, obscene, indecent or that attacks human dignity, especially concerning sex, race or creed;
   e. transmit unsolicited commercial and / or advertising material ("spamming"), as well as allowing your resources to be used by third parties for this activity;
   e. damage, destroy, attempt to access data without authorization or violate the privacy of other users, including the interception or disclosure of passwords, confidential cryptographic keys and any other "personal data" as defined by the laws on the protection of privacy;
   f. carry out activities on the internet that negatively affect the regular operating activities of the internet or restrict its usability and the performance for other users;
   g. carry out on the internet any other activity prohibited by the Law of the State or International law.
4. Each user of the Internet service also undertakes to respect regulations and customs ("Netiquette") of use of the networks and network services accessed.

Article 12 - Access to the Network: credentials

1. Users access the institutional network using their own network credentials. Network credentials allow authentication to the internal network. The same credentials allow to freely authenticate themselves to the print queue of all enabled printers. During the first configuration, the staff of the Infrastructures Office, IT services and digital administration checks that the operating system of the device or of user devices is adequately updated and that an antivirus, which is also updated, is available.
2. For security reasons, it is possible to access the network with any personal device only if it has an updated operating system and if the operating system's production date has not exceeded the tenth year of life.
3. Guests are allowed to access the network using their *Eduroam* credentials if available.
4. Guests who request it can access the network called IMT-Guest with special credentials, easily set by any web browser. For security reasons, the IMT-Guest network is separated from the internal network because no security checks are carried out on guests' devices. All the user devices that do not pass the security checks to access the network referred to in paragraphs 1 and 2 in this article are also connected to the IMT-Guest network.
5. No type of technical support is guaranteed for the connection on guests' devices, especially those that are particularly dated and/or without any updated antivirus programs.
6. The username of the credentials is specified in the name.surname form followed where requested by an @ sign and the authentication domain (e.g. name.surname@imtlucca.it); in case of homonymy, the username follows the next numbering (e.g. name.surname1).

Article 13 - Access to the Network – recording traffic logs

1. The details of the traffic generated in the internal network are stored in the form of anonymous *logs* on the appropriate device and the logs are stored for a period of 200 (two hundred) days.
2. The details concerning the authentication to the network are stored on the servers that deal with authentication and stored for a period of 200 (two hundred) days.
3. Security logs of network devices are available on a dedicated server.
4. The user must keep in mind that no registration of the content of the communications is made in any way and that all the logs are accessible only by system administrators.

Article 14 - Access to the Network – automatic filters

1. Automatic recognition filters are active on the network that prevent the execution of some *Peer to Peer* software that is excessively harmful from the point of view of bandwidth usage and whose general use is the download of material protected by copyright.
2. Automatic recognition filters are active on the network that prevent the running of software used to bypass the filters referred to in the previous paragraph.
3. For study and research purposes, computers are available to access the network without any block.

Chapter 4 Access to the School's information system

Article 15 - Access to the information system

1. Users access the School's information system through their own network credentials. Access to the information system is available from any public location connected to the Internet.
2. The credentials to access the School's information system are automatically created by the software management contracts.
3. The information system credentials are also used to identify the user to publicly accessible services, such as the Eduroam network, the *IDEM* federation and the *proxy http* for web browsing.
4. The same conditions of the guest network apply to the Eduroam network available on the premises of the School.

Article 16 - Access to the information system – recording of authentication logs

1. The registrations of the authentications to the services accessed through university credentials are available on dedicated servers and stored for a period of 200 (two hundred) days.
2. Authentication logs are accessible by system administrators.

Chapter 5 Final provisions

Article 17 - Personal use of telematic services

1. Reasonable use of your credentials for private and personal purposes is allowed, provided that, in addition to what is indicated in the previous points, such use:
   a. is not the direct or indirect cause of disservices of the processing systems;
   b. is not the cause of additional expenses to the School;
   c. does not interfere with the user's work activities or with their other obligations to the School.

   The user is informed of the fact that the School will consider, for the purposes of any inspections, all the e-mail messages and the network traffic managed by him/her as strictly related to the use of the service for work purposes. The School therefore assumes that the user decides to use his/her credentials for personal purposes having firstly and carefully evaluated the opportunity.

Article 18 - Service revocation

1. The User acknowledges and agrees that the School may revoke credentials in the event of inactivity for a period of more than six months. The revocation of the credentials involves the deletion of data.

Article 19 - Sanctions

1. In the event of abuse or violation of these regulations, or other regulations of the School, depending on the seriousness of it, and subject to the consequences of criminal, civil and administrative or disciplinary nature, the following penalties may be imposed:

a. the limitation and even total non-access to the network from a minimum of one week to a maximum of six months;

b. the revocation of all credentials with the consequent deletion of data.

2. The sanctions are imposed by the Administrative Director on the proposal of the Infrastructures Office, IT services and digital administration.

3. In the event of notice of abuse and danger of delay, the Administrative Director may order the immediate cessation of the activity causing the abuse by adopting the necessary measures to prevent the abuse from being led to further consequences.

Article 20 - School obligations and liability limits

1. The School undertakes to use the data provided by the user for the sole purpose of providing and managing the service and to implement all that is in its power to protect the user's privacy. The School provides for the preparation and dissemination of the information, pursuant to Article 13 of Legislative Decree n.196/2003 to the activation of the services.

2. The School implements all the measures of its competence deemed necessary and sufficient to minimize the risk of loss of information; however, it is not liable in any way and is relieved of any liability and obligation in relation to any deletion, damage, failure to send/receive or the omission of the contents, resulting from faults and/or malfunctions of the management equipment and/or generally of the service itself.

Article 21 - Modifications to these regulations

1. Modifications to these regulations deriving from new laws and regulations will be adopted with a specific Decree of the Administrative Director and communicated to the Board of Directors in the first possible meeting.