IT Policy

– for students –

Version/Date	2.0/ August 18, 2016 replaces version 1.0 (09. January 2009)	
Status	Approved by:	
	Robert Wilke	Antje Niebuhr
	Head of IT	Data Protection Coordinator
Author/Contact Person	Robert Wilke	
	Head of IT	

Table of contents

1 Introduction

Students (users) receive personalized IT login data (account) and the current valid version of the IT Policy at the start of their studies. The IT Policy is publicly available at http://it.esmt.org/topic/policies.

This IT Policy is considered accepted by the user as soon as he or she uses ESMT Berlin information technology for the first time.

Questions regarding the IT Policy may be addressed directly to the Head of IT (Robert Wilke, +49 30 21231-1080, robert.wilke@esmt.org).

Definitions

Phrase	Meaning
IT environment	entirety of hardware, software and application landscape (even cloud based) of ESMT
IT equipment	stationary equipment (PC, printer/ copy machines, surf stations) and mobile equipment (laptops/ notebooks, mobile/ smart phones, tablets, etc.)
IT resources	entirety of IT equipment, IT environment, IT services and staff

2 Purpose and Scope

The objective of this IT Policy is:

- to provide users an effective, flexible and safe IT environment
- to guarantee the faultless operation of the IT resources considering also restrictions/ limitations and regulations by law
- to increase the transparency of the conditions of the use of IT within ESMT and corresponding controlling measures
- to protect the personal rights of the users
- to protect data relevant to the company and the individual
- to make users familiar with the rules and conditions to be obeyed

Compliance to this IT Policy is mandatory for all students.

3 General Guidelines

3.1 Tenets of behavior

Any and every intentional and conscious use of IT that could harm ESMT's interests, public reputation, or license agreements, that could damage the company-internal network or that is in direct violation of applicable laws and regulations or the IT Policy is prohibited. This is especially true of:

- the retrieval and distribution of content that infringes upon personal rights, copyrights or applicable laws and regulations
- the retrieval or distribution of offensive, libelous, anti-constitutional, violence glorifying or pornographic statements or pictures

ESMT reserves the right to block (black-list) specific internet content that does not conform to these tenets of behavior.

3.2 Bring Your Own Device (BYOD)

Students working with their own equipment (BYOD) are fully responsible for their equipment. ESMT IT is responsible for the functionality of the ESMT IT environment.

3.3 Private use of ESMT IT resources

Private use of IT resources will be tolerated on a small scope if it does not interfere with daily business and or the availability of IT services

Within the scope of private use, no commercial or other business-related purposes should be pursued.

A differentiation between studies-related and private use cannot be technically made within the systems ESMT uses. Accordingly, Article 3.8 "Log files, controlling, data privacy" applies to both studies-related and private use (see also 5.3 Email)

With the private use of ESMT resources the employee expressly accepts, that private data might be visible during support activities of the IT department or contracted third parties, when reading log files, resetting passwords, etc.

3.4 Handling of IT equipment owned by ESMT Berlin

Every user is required to treat the equipment that has been put at his or her disposal carefully. Defects should be reported immediately to the IT department.

With the exception of mobile equipment, it is not allowed to move the location of ESMT equipment within ESMT. This applies mainly to printers, fax machines, copiers, surf terminals, etc.

3.5 Handling of IT equipment not owned by ESMT Berlin

Infrastructure and equipment not belonging to ESMT or managed by ESMT's IT department, e.g. private PCs, notebooks, routers, switches, printers, etc. will automatically be recognized as "external" components and will only have limited/ restricted access to IT Services and resources. These restrictions are due to data protection and data security reasons. (see also section 5.2 Network-/Internet access)

3.6 Software use on equipment owned by ESMT Berlin

An overview of current software including restrictions on volumes is published on the ESMT Intranet under "IT". The software applications on this list have been tested for their stability and security within the system landscape. The stability of the system can be put in danger through the installation and use of software that has not been tested. For this reason, additional software should only be installed on ESMT standard PCs/ notebooks and in coordination with the IT department.

3.7 Accounts and password guidelines

Each user is responsible for the secrecy of his or her access credentials (account information and passwords). Password policies and complexity guidelines are activated and documented at ESMT's Intranet under "IT".
The user is obliged to "lock" access to the computer whenever he or she leaves the workplace (e.g. account logoff or screen lock).

3.8 Log files, controlling, data privacy

Connection data for email and internet access is saved in a log file with the date, time, and addresses of the originator and recipient, as well as the transferred amount of data.

A differentiation between studies-related and private use cannot be technically made within the systems ESMT uses (see also 5.3 Email).

All log files are subject to the German data privacy regulations.

ESMT assigns employees of the IT department the status of system administrator. These persons have signed the corresponding obligation to respect data privacy. Nobody is allowed to put himself in a position of a system administrator or a comparable status.

Log files will be used only for the following purposes:

- analysis and correction of technical problems
- guarantee of system security
- controlling of network capacity, optimization of the network and applications
- statistics of the total usage volume
- random sampling of visited websites for controlling of misuse (This sampling will not be connected to individual accounts.)

Random sampling and other analyses of the log files will not be used to determine performance or behavior of singular individuals. The access to log files for random examination shall not take place without previously arranged and explicit instruction. The log files will only be accessed by the system administrator(s).
Log files will be deleted after 4 years at the latest.

4 Sanctions in case of violation of these guidelines/ misuse

Experience has shown that most infractions to the IT Policy occur unknowingly or due to technical deficiencies. For this reason, those who infringe upon the IT Policy, as far as it possible to discover this person, will usually first be informed of the misuse and asked to refrain from misuse in the future or to stop or uninstall programs causing the technical deficiencies.

In case of repeated conscious misuse, or malicious act the access authorization may be temporarily revoked (user account deactivated).

In case of a blatant infringement upon license agreements, IT may demand that the affected software and the data created with it be deleted.

Should the infringements upon the IT Policy pose a danger for data, availability of IT services, or ESMT's interests or public reputation, IT is authorized to (temporarily) deactivate the corresponding user accounts or to exclude the equipment from the network.

In case of suspected misuse or unauthorized use of information technology, i.e. in contradiction to the IT Policy, measures for closer examination may be initiated. This would take place together with ESMT's data protection officer or data protection coordinator and a system administrator and, if necessary, another person named by the management board. The person under examination would be informed about the measures and would receive a report.

ESMT reserves the right to other, including legal, procedures in case of infringement upon the IT Policy. The President of ESMT will be informed of any and all criminally liable violations.

5 IT service overview

The possession of an account is a prerequisite for the use of IT services.

Accounts and their associated licenses will be made available exclusively for the duration of study (unless, in individual cases, otherwise communicated).

The following overview of IT services does not illustrate a complete IT service catalogue and is limited to the most important services.

Agenda	
Legend	Meaning
●	service
◑	service offered in reduced scope (see corresponding subsequent chapter)
○	no service

IT services	ESMT standard equipment	Other equipment
IT Support	●	○
Network and internet access	●	◑
Email	●	◑
Print/copy/fax services	●	◑
ESMT specific software	●	◑

5.1 IT Support

Please always send incidents or requests to IT Support as the single point of contact.

Telephone IT Support	+49 30 21231-**1234**
Email IT Support	it.support@esmt.org
IT Support service times (workdays)	Monday - Friday: 8:00 a.m. – 6:00 p.m.

All incidents and requests will be prioritized by the IT Support team and then processed accordingly. Incidents impeding daily business, e.g. concerning events in the Learning Center, will be given top priority.

5.2 Network / internet access

ESMT provides two primary networks:

- the company network with access to all relevant applications and IT services
- guest network for event participants, students, and guests

These networks may be accessed with WLAN or with a network cable.

Connecting devices are automatically assigned to a network based upon the registration status of the equipment (PC, notebook, etc.). Private or non-ESMT equipment can only use the guest network.

5.3 Email

Students are provided a lifelong email account from ESMT for correspondence that is directly and indirectly related to the student's studies. ESMT Berlin reserves the right to provide email service through a third party. In such cases ESMT Berlin ensures that an agreement with the third party service provider has been made, in which it is required that German data privacy laws are upheld.

It is generally prohibited to send or forward objectionable email messages that conflict with Part "3.1 Tenets of behavior " or mass emails that have not been approved (suspicion of SPAM).

Incoming emails are checked for SPAM characteristics and, if applicable, automatically quarantined or sent to the user's "Junk E-Mail" folder. Despite careful examination, it cannot be guaranteed that only SPAM mails will be quarantined/ land in this folder. For this reason, users should check the "Junk E-Mail" folder regularly and read SPAM-suspicion notifications carefully.

5.4 Print/ copy/ fax services

The possibility to print, copy and fax has been made available with so-called multi-purpose devices.

On ESMT's Intranet under IT, you can find more information about:

- printer locations
- instructions for use of the printers

5.5 ESMT specific software

An overview of the current required and offered scope, related use, and period of availability of studies-related software will be presented in the introduction presentation held at the beginning of the student's studies.