Information and Communications Technology Guideline

Preliminary remarks

The safeguarding of electronic communication represents an excellent basis for both the fulfilment of the tasks of all JACOBS UNIVERSITY (hereinafter also referred to as JACOBS) employees and the guaranteed provision of the best possible study conditions for all students. This guideline regulates the rights and duties of users and administrators and is to be observed so that the ICT (information and communication technology) resources and services of the IRC may be used efficiently, transparently, securely and as far as possible without disruption. Its purpose, in the context of basic rights and in the spirit of the freedom of research and teaching pursuant to Article 5 of the Basic Law of Germany, is to implement the legal requirements relating to data protection, telecommunications and telemedia that must be observed by JACOBS in its provision of telemedia services for all users.

FIRST SECTION: GENERAL POINTS

1. Scope and definition of terms

The guideline applies to all users of ICT resources at Jacobs University: that is, to employees, students, professors, scientific staff, student ancillary workers and guests.

(1) *ICT Resources*

All hardware and software, irrespective of the place of use, as well as all services of the IRC (the list is not exhaustive).

(2) Services

Services comprise all the technical and human resources services named in this guideline which are used for the purpose of the provision and maintenance of the IT and telecommunications resources.

(3) *Telemedia*

Telemedia in the context of this guideline are all those media and protocols that permit electronic communication, with particular reference to the Inter-/Intranet but also including telecommunications services such as e-mail and telephony (including VoIP).

(4) Employees

Employees are all those users who work for JACOBS, irrespective of the nature of the legal relationship with JACOBS (employees, student ancillary staff, teachers, visiting lecturers etc).

(5) Impermissible contents and types of use

Contents and types of use which are either illegal or declared impermissible by this guideline, with particular reference to the following:

a. *Impermissible contents are those which*

- Are in violation of provisions contained in the German Criminal Code,
- Glorify war,
- Clearly pose a serious moral risk to children or young people,
- Represent people who are dying or who are or have been subject to serious physical or mental suffering in a way that is injurious to their human dignity, and disclose actual events without the existence of a clearly justifiable interest in this particular form of reporting; whether or not consent has been given is irrelevant,
- Are in any other way injurious to human dignity,
- Are in violation of legal provisions in respect of data protection, personality rights, copyrights or criminal law,
- Include racist, sexist or pornographic statements and images.

b. *impermissible types of use are*

- The harassment or threatening of other users
- The disruption to, or prevention of, the use of IT activities by other users
- The unauthorised access to or unauthorised use of IT services
- Damage to, or impairment of, Jacobs resources
- Prohibited commercial activities

Contents and types of use which are verifiably being used for the purpose of scientific research and teaching as defined in article 5 of the Basic Law of Germany are unaffected by this.

SECOND SECTION: SERVICES

2. Access

(1) To the extent that the technology allows, JACOBS grants all users access to the ICT resources by various technical means (Ethernet, WLAN, UMTS etc.) but cannot guarantee permanent access to same. The use of access rights may be logged; please refer to the annex for details. The connection by users of private terminals is permitted.

(2) The unauthorised use of JACOBS resources is prohibited and can be blocked by technical means. Personal access rights may be used only by the individual to whom they have been granted and may not be passed on to others.

3. Use of e-mail

Technical measures are taken to ensure that access to individual mailboxes is restricted in each case to the persons entitled to access them. Regulations governing employee substitution (cf. section 13) are unaffected by this.

(2) E-mails and their attachments are as a matter of course automatically scanned for harmful content (malware) and may automatically be deleted by the IRC if they contain contents or attachments that are impermissible or might impair network security. Sender or target addresses of e-mails can also be blocked without any requirement to inform the sender or recipient thereof, especially if there is particular justification (e.g. the blocking of attacks on users or infrastructure) for doing so.

(3) Spam, bulk or similar mass mails directed to JACOBS users can be automatically identified before they reach their addressees.

(4) IRC administrators have the right to limit the capacity of mailboxes in order to vouchsafe the smooth operation of the system.

All the security measures named above are carried out in the framework of the confidentiality of telecommunications pursuant to § 88 of the German Telecommunications Act without any disclosure of the contents of e-mails.

4. Content publishing

(1) Users are responsible for the legality of publishing contents throughout the JACOBS organisation or globally (Internet). When publishing contents, users must observe the provisions of copyright law and rights of use, as well as the requirement to safeguard operational secrets and similar obligations to observe secrecy. Impermissible contents as defined in section 1 (5) may not be published.

(2) JACOBS reserves the right to take central measures to block the provision of impermissible or illegal contents or those that pose an operative risk.

(3) If private home pages are published in this connection, these will be deleted 90 days after the user's departure from JACOBS.

5. Internet use

(1) No filtering of content takes place, nor does JACOBS use technical or other measures to check whether users are (legally or contractually) entitled to access particular contents.

(2) The users themselves are solely responsible for the legality of access; this applies also to contents which minors are not permitted to access. §§ 8 and 9 of the German Telemedia Act (Telemediengesetz – TMG) apply additionally in this case.

(3) The use of peer-to-peer software or similar applications is prohibited and can be prevented by JACOBS by technical means.

(4) JACOBS reserves the right to take central measures to block the provision of impermissible or illegal contents or those that pose an operative risk.

6. Storage of contents

(1) Each user is allocated storage space on the JACOBS servers to which he or she alone has access rights and which offers limited scope for the storage of private contents (personal directory). The size of the personal directory may vary and depends on the capacity utilisation of the total storage media provided in each case. JACOBS reserves the right to change the volume of the storage space. Contents may automatically be checked for harmful contents, although private contents are not disclosed in the process.

(2) Impermissible contents as defined in section 1 (5) may not be stored.

7. Leaving JACOBS

Before a user leaves JACOBS he or she must ensure that no private contents remain on data storage media and telemedia services. Private contents that are left on the data systems, even given the possibility of deleting them, will be deleted.

THIRD SECTION: ADMINISTRATION AND LOGGING

8. Administration

(1) All members of staff at the central data processing unit are informed of the requirement pursuant to § 88 TKG to pay particular attention to the safeguarding of telecommunications secrecy; telecommunications secrecy is guaranteed. Pursuant to § 88 section 3 TKG, administrators may obtain information concerning the content or more detailed particulars of telecommunication activities only for the purpose of the business-related provision of telecommunications services, including the protection of their technical systems, and only to the extent required to do so. All administrators are under obligation to maintain data secrecy pursuant to § 5 of the Federal German Data Protection Act (Bundesdatenschutzgesetz – BDSG).

(2) Mailboxes and central data storage facilities are set up centrally by JACOBS systems administrators, who are likewise responsible for the administration of telemedia services. The right to decentralise individual administrative tasks is reserved.

(3) Administration includes logging and further activities listed in the Annex (in the version currently in force).

9. Use of log data

(1) Logging is carried out in order to ensure that the services operate flawlessly and reliably in the interest of all users. This includes

- The rectification of system errors,
- The protection of infrastructure and services from attacks and unintended malfunctions,
- The administration of network and application resources,
- The generation of statistics,
- The investigation and resolution of misuse, i.e. the identification and prevention of impermissible types of use pursuant to § 1 (5),
- The optimisation of the service.

(2) No general user-specific logging of user data is carried out.

(3) All log data are deleted after a maximum of one week unless such data are required for invoicing purposes or the execution of the measures set out in section 3.

(4) If reasonable grounds for suspicion arise concerning impermissible contents or types of use pursuant to section 1 (5), specific data that may be related to individual persons can be logged and evaluated for the purpose of further investigation. This is time-limited to a period of up to four weeks. The officer responsible for operative data protection is informed of this. The person in question is informed once the measure has been completed. Any data not required for this purpose are deleted.

(5) If this evaluation provides evidence that impermissible contents have been accessed, proceedings under the terms of labour or civil law may follow.

(6) If this evaluation provides evidence that impermissible contents have been accessed, criminal investigation authorities may in addition be brought in; the officer responsible for operative data protection will be informed of this.

FOURTH SECTION: SPECIAL REGULATIONS FOR EMPLOYEES

10. The secure handling of data and IT resources

All JACOBS employees are required to treat JACOBS data in confidence, irrespective of whether these are personal data or such data as are to be kept secret or treated in confidence for internal operative reasons. Personal data for which JACOBS is responsible and confidential operative data may not be stored on private terminals.

Confidentiality in dealing with data may be assured by

- The encryption of e-mails
- The use of complex passwords
- Maintaining the confidentiality of passwords and other access protection mechanisms
- The use of hardware and software provided by JACOBS
- The use of secure communication channels

11. Private use by employees of telemedia

(1) The private use by employees of telemedia is permissible to a limited extent, whereby it is to be noted that private use is always subordinate to the operative interests of JACOBS UNIVERSITY. The following regulations apply to the use by employees of the different media.

(2) No monitoring of performance or conduct (e.g. through the creation of communication profiles) takes place.

(3) The private use of JACOBS resources may be prohibited.

(4) The use of JACOBS services for private purposes presupposes that the users have given their express consent to the framework conditions described in Section 2. Such a declaration of consent may be given in writing or electronically. If this declaration of consent is not made, it will be assumed that the JACOBS services are being used exclusively for professional purposes.

12. Storage of contents

Contents must in all cases be stored on the central servers made available for this purpose; local storage is permissible only in exceptional circumstances (e.g. if, at the time, no network or server is available). If contents have been locally stored, they are to be stored on, or moved to, servers as soon as technically possible.

13. Use of e-mail by JACOBS employees

Privately sent and received e-mails and their attachments may only to a limited extent be stored on servers or workplace computers. These are subject to the terms of confidentiality of telecommunications in accordance with § 88 TKG.

(2) In the event of foreseeable absence (e.g. holiday or business travel), the absent member of staff should arrange for an automatic response text (Out-of-Office assistant) to be sent to the sender of the e-mail in which reference is made to the absence of the recipient or another e-mail address is stated. A member of staff being represented can arrange for e-mails to be automatically forwarded to his or her substitute.

(3) In the event that the absent member of staff has not made any substitution arrangements for either planned or unforeseen absence, JACOBS can (when prompted to do so by the member of staff's superior) itself set up an Out-of-Office assistant.

14. Use of the Internet by JACOBS employees

Contents downloaded from the Internet for professional purposes may be stored on a server or workplace computer only if required for professional reasons.

15. Telephony/Voice-over-IP use by JACOBS employees

(1) The user must use the cheapest possible connection method. This means in particular the use of VPN services and internal company numbers and the selection of the cheapest available technology. Connections that bring about additional charges (e.g. WAP, GPRS, UMTS) are to be restricted to the absolute required minimum.

(2) JACOBS can limit the numbers which may be called using particular connections.

(3) JACOBS can provide unified messaging functionality for computer access to telephone functions (including but not limited to configuration, fax, answering machine/voicebox, e-mail forwarding, dialling from a computer, SMS, instant messaging, video conferencing, desktop sharing). The provision of these is voluntary and may be subject to restriction. The initiation of communication links takes place only with the consent and active participation of the user.

(4) The user is responsible for the security of the configuration that relates to him and the prevention of access by third parties.

(5) Contents stored on telecommunications servers (answering machines and fax) are automatically deleted after 1 month.

JACOBS reserves the right when required by operational necessity to change the configuration of telephones, answering machines and unified messaging. Stored contents can be deleted in the process; for this reason it is not recommended to store private contents.

(7) Individually itemised connections are always abbreviated by removing the last 3 digits.

(8) Private telephone conversations are to be identified by dialling the prefix “8” (for outside line). The user responsible will be required to pay the excess costs for telephone calls that result in unusually high charges.

16. Termination of the employment relationship

For employees, the deletion requirements in section 7 apply with the following framework conditions:

- The datasets left on JACOBS equipment are to be passed on in an orderly manner by the departing member of staff to his or her superior or, where applicable, a successor; the latter will be granted unrestricted access rights to the datasets left on the equipment (including telephony, unified messaging etc.).
- If so requested by the departing member of staff, a time-limited redirect function for personally addressed e-mails can be set up subject to the consent of his or her superior and as long as there are no operational reasons not to do so. This redirect function can be cancelled at any time.
- Any remaining data can be deleted at the latest 6 months after the departure of the employee in question.

FIFTH SECTION:

17. Effective date

This guideline comes into force at the time of its announcement or posting on the notice board.

Bremen, dated April 1st, 2012

(J. Treusch, President)

Annex: Administrative functions of the IRC:

Logging

E-mail

- Incoming and outgoing e-mails (sender and addressee e-mail addresses, message ID, name and IP address of the computers involved, size of the e-mail)

Internet

- The source and target addresses,
- The communication ports,
- Date, time and duration of the access, and
- The volume of data exchanged via the communication link

Telephony

- Itemised connection lists with abbreviated destination numbers (including the outgoing number and the start and end of the call)
- For the purposes of invoicing and ensuring proper use

System

- The allocation of an IP address to a MAC address via the DHCP service (IP address, MAC address, time stamp),
- The link-up and link-down of a MAC address at a switch port (MAC address, switch port, time stamp),
- Login and logout in the case of interactive server services (username, success/failure, time stamp),
- VPN connection and disconnection (abbreviated login, time stamp),
- Data retrieval for server services: Log data corresponding to the data format of the service in question

Further administrative functions

- NAT – Network Address Translation (also known as “masquerading”)
- Port filtering – to prevent the spread of viruses and other harmful software.
- Peer to Peer identification and blocking
- Traffic Shaping – to guarantee the availability of stipulated bandwidth
- The termination of processes to ensure system availability

Declaration of consent

Private use of Jacobs services (for employees only)

JACOBS grants me the use of Jacobs services for both the fulfilment of work-related tasks and limited private purposes. The current guideline on the use of information and communications services contains more detailed regulations.

With this declaration I give my consent to the following:

- The logging of private access
- The scanning of all incoming e-mails for defective content and content that might be harmful to the Jacobs network, the identification and, where applicable, deletion of e-mails without notification of the user
- The blocking of access to, and the offering of, impermissible contents
- The logging of ICT use in the scope described in detail in the guideline
- The further processing and/or deletion of data left on the server after my departure.

I can withdraw this consent at any time. In this event I can however continue to use the Jacobs services exclusively for professional purposes.

ONLY THE GERMAN VERSION IS BINDING.

First name, surname

PLEASE USE NEXT PAGE.

CampusNet username

Division/department

Date Signature of member of staff

Einwilligungserklärung

Private Nutzung der Jacobs-Services (nur für Beschäftigte)

JACOBS stellt mir die Nutzung der Jacobs-Services sowohl zur Erfüllung von Arbeitsaufgaben sowie zur eingeschränkten privaten Nutzung zur Verfügung. Näheres wird durch die jeweils aktuelle Richtlinie zur Nutzung von Informations- und Kommunikationsdiensten geregelt.

Mit dieser Einwilligung stimme ich zu, dass

- private Zugangs-Nutzungen protokolliert werden können
- alle eingehenden Emails auf schadhafte Inhalte und weitere für das Jacobs-Netzwerk schädliche Inhalte gescannt, gekennzeichnet und ohne Benachrichtigung des Nutzers ggfls. gelöscht werden können
- der Zugriff auf und das Anbieten von unzulässigen Inhalten gesperrt werden kann
- die ICT-Nutzung in dem in der Richtlinie näher beschriebenen Umfang protokolliert werden kann
- auf den Servern verbleibende Daten nach meinem Ausscheiden weiter verarbeitet und/oder gelöscht werden können.

Die Einwilligung kann ich jederzeit widerrufen. In diesem Fall kann ich die Jacobs-Services jedoch ausschließlich zu beruflichen Zwecken verwenden.

PRIONTU CHOWDHURY

Vorname, Nachname

pchowdhury

CampusNet-Username

Electrical and Computer Engineering

Bereich/Abteilung

06.09.2021

Datum Unterschrift Mitarbeiter/in