USAGE GUIDELINES FOR WEIHENSTEPHAN-TRIESDORF UNIVERSITY OF APPLIED SCIENCES IT SYSTEMS

dated 22 May 2013

Preamble

Weihenstephan-Triesdorf University of Applied Sciences (referred to as HSWT and hereinafter also as 'the operator') operates an information technology infrastructure (the IT infrastructure – see Section 1). The IT infrastructure is integrated into the German Science Network (Deutsches Wissenschaftsnetz – WiN) and hence into the global internet.

These usage guidelines regulate the conditions under which the service can be used, the rights and obligations of users and the duties of the operator.

These usage guidelines:
- are founded in the legally prescribed role of universities and in their mandate to safeguard academic freedom,
- set out basic rules for the proper operation of the IT infrastructure,
- make reference to third-party rights that must be safeguarded (e.g. regarding software licences, obligations to network operators, data protection matters),
- commit the user to proper conduct and to economic and ecological use of the resources provided,
- specify possible measures that the operator may take if these usage guidelines are infringed.

Section 1: Scope

These usage guidelines apply to the IT infrastructure provided by HSWT, consisting of computing systems (computers), communications networks (networks), services and other auxiliary aspects of information technology.

Section 2: Users and roles

1. The IT resources referred to in Section 1 are available to members of Weihenstephan-Triesdorf University of Applied Sciences to perform tasks relating to research, teaching, management, training and continuing education, public work and the public image of universities and for any other tasks described in Article 2 of the Bavarian Universities Act.
2. Other persons, specifically members of other universities, organisations and institutions, may also be permitted to use the infrastructure.

Section 3: Formal user authorisation

1. Anyone wishing to use the IT resources referred to in Section 1 requires formal user authorisation from the system operator responsible. This does not apply to services that are set up for anonymous access (e.g. information services, library services, short-term guest IDs).

2. The system operators are
   a) the Computer Centre in the case of central systems,
   b) the responsible organisational unit (departments, central facilities, university administration) in the case of peripheral systems.

3. Formal user authorisation includes the following user data:
   a) operator or organisational unit supplying the user authorisation;
   b) systems for which user authorisation is provided;
   c) user: name, address, telephone number (and matriculation number for students) and, where relevant, membership of an organisational unit of the university;
   d) broad details of reasons for use, such as education/teaching, administration, student project, dissertation or thesis, research;
   e) declaration of agreement that the operator may alter user authorisations and user data such as passwords in order to protect the operation. The user must be made aware of this immediately;
   f) declaration that the user accepts the usage guidelines and agrees to the storage and processing of personal data;
   g) records for internal information services of Weihenstephan-Triesdorf University of Applied Sciences (e.g. information server website, telephone directory).

The relevant data protection regulations must be observed. The system operator may process further data only to the extent that it is necessary for the provision and management of user authorisation.

4. The system operator responsible may make provision of user authorisation conditional on evidence of specified skills relating to the use of the system. User authorisation may be provided for a limited or for an unlimited period and will terminate at the latest on termination of membership of Weihenstephan-Triesdorf University of Applied Sciences.

5. User authorisation may be refused if
   a) it does not appear possible to guarantee that the applicant will comply with his or her obligations as a user;
   b) the capacity of the system whose use is being requested is insufficient for the intended work, due to current utilisation levels;
   c) the intended use is not consistent with the purposes specified in Sections 2 (1) and 4 (1);
   d) the system is clearly unsuitable for the intended use, or is reserved for specific purposes;
   e) the system to be used is connected to a network that is required to satisfy special data protection conditions and no objective reason for the requested access is apparent;
   f) it is anticipated that the requested use will interfere disproportionately with other authorised uses.
6. User authorisation applies only to work related to the requested use.

Section 4: Obligations of the user

1. The IT resources referred to in Section 1 may be used only for the purposes specified in Section 2 (1). Use for other purposes, and specifically for commercial purposes, will be allowed only on request and subject to a fee.

2. The user is obliged:
   a) to ensure that he or she uses the available resources (workstations, CPU capacity, disk space, bandwidth, peripheral devices and consumables) in a responsible, economic and ecological manner. Workstation computers and printers must be turned off outside working hours, unless there are important official reasons for not doing so;
   b) to refrain from foreseeable interference with the operation and to take all steps to avoid doing anything that might cause damage to the IT infrastructure or harm to other users;
   c) to refrain from any type of misuse of the IT infrastructure;
   d) to use only user IDs that he or she is permitted to use; it is not permissible to pass IDs and passwords on to others;
   e) to protect access to the IT resources by using a password that must be kept secret, or by an equivalent process;
   f) to take precautions to prevent unauthorised third parties from gaining access to the IT resources; this includes in particular blocking access to the system, logging off or switching off when leaving the workstation;
   g) when using computers of other operators, to observe fully their user and access guidelines;
   h) when using software (sources, items), documentation and other data, to observe statutory regulations (copyright);
   i) to keep themselves informed of the conditions under which software, documentation and data, including any which may be being used under licensing agreements, are made available, and to adhere to these conditions;
   j) in the case specifically of software, documentation and data, unless expressly permitted, neither to copy nor pass these on, nor to use them for purposes other than the permitted purposes, and specifically not for commercial purposes.

The user will bear full responsibility for all activity carried out using his or her user ID, including that carried out by third parties in cases where he or she has at least been negligent in allowing access. Contraventions may give rise to claims for damages (Section 7).

3. The IT infrastructure must, of course, be used only in a legally correct manner. Attention is expressly drawn to the fact that the following activities in particular are punishable under the relevant sections of the German Criminal Code (StGB):
   a) appropriation of the passwords of others and of data (StGB Section 202 a)
   b) unauthorised alteration, deletion, suppression of data or rendering it unusable (StGB Section 303 a)
   c) computer sabotage (StGB Section 303 b) and computer fraud (StGB Section 263 a)
   d) distribution of propaganda from unconstitutional organisations (StGB Section 86) or of racist ideas (StGB Section 131)
   e) distribution of certain forms of pornography over the network (StGB Section 184 para. 3)
   f) defamation such as libel or slander (StGB Sections 185 et seq.)
The operator reserves the right to take steps under criminal or civil law (see Section 7).

4. The user is forbidden, except with the permission of the operator responsible:
   a) to interfere with the hardware installation;
   b) to alter the configuration of the operating systems or network. The right to install
      software is covered by specific regulations depending on local and technical
      circumstances.

5. The user is obliged to obtain the agreement of the system operator before
   commencing any undertaking that involves the processing of personal data. This will
   not affect any obligations arising from provisions of the German Data Protection Act.

6. The user is forbidden to read and/or make use of messages intended for other users.

7. The user is obliged:
   a) to adhere to any additional usage conditions, guidelines and guidance on usage
      issued by the operator;
   b) when using the computers and networks of other operators, to adhere to their usage
      and access guidelines.

Section 5: Duties, rights and obligations of the system operator

1. Every system operator will document all usage authorisations provided. The
   documents must be preserved for a minimum of two years following expiry of the
   authorisation.

2. The system operator will contribute in an appropriate way, as agreed with the
   president and the data protection officer of the university, to the prevention and
   detection of misuse.

3. The system operator has the right in particular:
   a) to monitor the security of systems and passwords regularly using suitable software
      tools, in order to protect its resources and users’ data from attack by third parties;
      users must be promptly notified of this;
   b) to document and analyse the activities of users, insofar as this is for the purposes of
      accounting, resource planning, protecting other users’ personal data, monitoring the
      system or tracing faults or infringements of the usage guidelines and of statutory
      regulations;
   c) in the case of suspected infringements of the usage guidelines or of criminal law
      regulations, and on condition that the principle of dual control and the obligation to
      document activities are observed, to inspect user files and mailboxes or to keep a
      detailed record of the user’s network usage through the use, for example, of network
      sniffers; such inspection must be agreed with the president and documented and the
      affected user must be informed immediately once the purpose has been met;
   d) if the suspicion of punishable activity is confirmed, to deploy measures for obtaining
      evidence such as key-stroke logging or the use of network sniffers.

4. The system operator has a duty of confidentiality.

5. The system operator will notify its users of a support contact person.

6. The system operator is obliged, when using computers and networks of other
   operators, to adhere to their usage and access guidelines.

7. Where operations make it necessary, the system operator may temporarily restrict
   use of the IT infrastructure or temporarily suspend individual usage authorisations. If
   possible, the affected users should be informed of this in advance.
8. If there are factual indications that a user has illegal content for use on the system operator’s infrastructure, the system operator may prevent further use until the legal position has been sufficiently clarified.

Section 6: Operator’s liability/exclusion of liability

1. The operator does not guarantee that the system’s functions will meet the specific requirements of the user or that the system will run without error or interruption. The operator cannot guarantee the integrity (in relation to destruction or manipulation) or reliability of data stored on its system.

2. The operator accepts no liability for loss or damage of any kind incurred by the user as a result of his or her use of the IT resources referred to in Section 1, unless it is the result of deliberate conduct by the operator or by persons the operator is using to fulfil its duties.

Section 7: User’s liability

1. The user is liable, subject to statutory provisions, for any detriment caused to the operator through misuse or illegal use of the IT infrastructure and usage authorisation or through the user’s culpable failure to meet his or her obligations under these usage guidelines.

2. The user is also liable for loss or damage arising from the use by a third party of the access and usage facilities made available to him or her, if he or she is responsible for such third party use and particularly where his or her user ID has been passed on to a third party. In such a case, the operator may demand from the user a usage fee for the use by the third party.

3. Insofar as the user can be held liable for them, the user must hold the operator harmless from any liability in cases where third parties make a claim for damages, neglect or other matters against the operator because of misuse or illegal conduct on the part of the user. The operator will enjoin the user in proceedings where a third party takes legal action against it.

Section 8: Consequences of misuse or illegal use

1. In the case of infringements of statutory regulations or of the stipulations of these usage guidelines, particularly those of Section 4 (Obligations of the user), or where the operator has suffered detriment through other illegal user conduct, the operator may restrict usage authorisation or withdraw it in whole or in part. In such cases it is irrelevant whether or not the infringement resulted in loss or damage. Where such infringements are serious or repeated, a user may be permanently excluded from the use of all IT resources referred to in Section 1.

2. The Computing Centre will make this decision in consultation with the Chancellor of Weihenstephan-Triesdorf University of Applied Sciences in relation to the full scope of these usage guidelines. The affected user will be given the opportunity to respond and to secure their data.
3. Infringements of rules relating to legal matters, employment law or service law, or of the stipulations of these usage guidelines, will be assessed under criminal and civil law. The system operator is obliged to refer apparently significant matters to the Chancellor of Weihenstephan-Triesdorf University of Applied Sciences for judicial assessment and, where relevant, for instituting appropriate further steps.

Section 9: Other regulations

1. Fees for the use of IT resources may be set in separate regulations.
2. For specific systems, the relevant system operators, in consultation with the Computing Centre and university management, may determine additional or different usage regulations where necessary.
3. Additional or different usage regulations may apply to some employees on account of service agreements or the stipulations of service or collective bargaining law.
4. Should parts of this user agreement be or become ineffective, this will not affect the validity of the remainder.
5. The competent court for any legal disputes arising out of this usage agreement is Freising.

Section 10: Effective date

These usage guidelines come into force on the day after publication.

Freising, 22 May 2013
University Management