Dresden International School Computer and IT Use Policy

Overview

This document specifies the important ground rules that students must follow when using computers, IT services and IT equipment provided by Dresden International School. Above and beyond everything, students must:

- use school computers and IT equipment respectfully and carefully,
- keep personal data and login data secret,
- not use school computers to download, duplicate, modify and/or distribute copyrighted materials (in accordance with German copyright law),
- not use computers to distribute illegal content over the local area network or through the internet,
- not use computers to distribute personal data (name, birth date, personal photos) of themselves, classmates or teachers to the public (for example, via the internet).

Please take the time to read through and understand this important document.

A. Use of computer and media equipment in the school

1) Scope of Application

The rules in section A are valid for the use of the computers, the computers' services, and the network located and accessed on Dresden International School campuses.

These rules also apply to any devices that are connected to the school computers or the network either provided by the school, the teachers or the students (for example, personal laptops, digital cameras, digital video equipment, USB sticks, etc.).

2) Authorized Use

Students are authorized to use available computers and laptops as designated by their teachers or school staff in accordance with the rules outlined in this policy document.

3) Login Information

a) All students may receive logins and passwords for access to the school's computer systems and school network.

b) Users must choose their own passwords. Passwords should be at least 8 characters in length, should not contain any identifying information and should contain a combination of letters, numbers and special characters.

c) When a student is finished using a school-provide computer, the student must log out.

4) Password Secrecy

   a) Students have the responsibility to protect the secrecy of their passwords. This means that a student must not give his or her login information to other people and must not log in to the computer system for other people. Students are expected to report when they notice other people using another person's login and password for access to the school's computer systems. The school administration has the right to deactivate any login that is suspected to be compromised.
   b) A student is not allowed to use someone else's username and password to access the school's computer systems and/or network.
   c) Students are not allowed to obtain passwords of other system users by any means.

5) Copyrighted Materials

   a) Students may not use the school computer systems and/or network to duplicate, distribute or alter copyrighted digital media without express written permission of the copyright holder or copyright administrative organization and permission of a teacher or school staff.
   b) Students may not use the school computer systems to circumvent copy protection (such as DRM) on digital media.
   c) Students may not store copyrighted material on the school's computer systems (for example, music, movie clips, images, software etc.). Copyrighted material may be deleted without notification.
   d) Students may not use their own devices to transmit copyrighted materials to other people's devices.

6) Computer Use for School Purposes Only

The school computer systems and network (e.g. computers, intranet, internet access, software, external devices, cameras, video cameras, printers, scanners, etc.) may only be used for school-related purposes. This rule applies during class, during break and lunch times, before school and after school.

7) Bring Your Own Device

   a) Students must bring a fully charged, functioning laptop to school in accordance with the BYOD requirements and bring it to all classes with the exception of physical education.
   b) Laptops must be charged at home. Students may not charge their laptop batteries in the school.
   c) Students must follow teacher instructions with respect to their personal laptops.

8) Device Use

a) Students must provide their own way of storing and backing up their school computer files. This can be accomplished, for example, by storing documents online, storing them on student owned laptops or on students' own USB sticks. The school will not provide any storage for students' computer files.

b) Students may bring other electronic devices to school in addition to their laptops (for example mobile phones, digital cameras, video cameras, etc.), but they may do so at their own risk. The school does not take any responsibility for loss, theft or damage of these items.

c) Students may not alter, damage, or otherwise attempt to corrupt school computers or the computers of other students, computer workspaces, external devices, the school network or software.

d) Students may not have food or drink near a computer or computing equipment.

e) After finishing using a school computer, a student should leave the workspace ready for the next person. This means that the student should remove all materials from the workspace, push the chair back in under the desk, and log out.

f) Students may not use school electronic devices (for example, video cameras, digital cameras, card readers, laptops, beamers, etc.) without the **permission** and **supervision** of a teacher or staff member.

g) In special cases, students may check out special electronic media devices for use off-campus and without teacher or staff member supervision. For these purposes, a different procedure applies and the student’s parents/guardians will be informed in advance in writing.

h) Students may not use devices to share assessment materials with other students unless explicitly instructed to do so by a teacher.

9) Damaged Items

a) In the case that an item of the school’s IT equipment (computer systems, network or devices) has been damaged, students should report the damage to a teacher or school staff member. In the case that a student has damaged an item, that student’s parents/guardians will be billed for the replacement or repair of the damaged item.

b) In the case that a student's laptop or other media equipment is damaged, the student's family has the responsibility to have the item repaired or replaced.

10) System Configurations

a) Students may not change the installation and configuration of the school computer systems (both hardware and software) and network.

b) Students may only restart computers with the permission of teachers or school staff.

c) Students may not access, modify, delete or destroy another user's files.

d) Students may not deactivate virus scanners and configured start-up processes.

e) Students may not install software on any school computing device.

f) Students may not introduce viruses, trojans, worms, root-kits, keyloggers, network sniffers, etc. to the schools computer systems and network.

11) Printing

a) Students may use the printers and copiers in the hallways, library and secondary technology lab to print out documents or to make copies.

b) Students will be issued one copy card which is needed to access the copiers and printers.

c) The copy card will contain a limited number of pages that can be printed or copied. Once a student's balance reaches zero, he or she will have to request additional copies.

d) The school reserves the right to charge fees or to turn off a student's copy card account in the case of excessive copying or printing.

e) If a student loses his or her copy card, a 2.00€ fee will be charged for replacement.

f) Students may not share their copy card with others.

12) Fees

a) Use of computers, IT and media equipment is currently available in the school without additional fees to the student. Students are expected to use the school computer systems and network respectfully and mindfully.

b) The school reserves the right to charge fees in the future for specific IT services in the schools. Notifications of fee changes will be announced in advance in writing.

B. Internet Access and Use

13) Prohibited Use

Students who access the Internet using school computers should avoid legally prohibited websites. Above all others, sites that have pornographic content, offer gratuitous violence, contain racist content, or in some other way violate Germany's *Jugendschutzgesetz****[1]*** are forbidden. In the case that a student accidentally accesses such a page, the student should report this to a teacher or staff member immediately.

14) School Web Filter

One of the ways that the school controls and monitors web access for students is via a web filter. Students may not attempt to bypass the school's web filter (for example, by attempting to use a proxy service).

15) Download of Internet Content

a. Students may not download copyrighted digital media.
b. Establishing and using file sharing networks is not allowed.
c. Downloading software and making that software available to others is not allowed.
d. Downloading large files (>100Mb) over the school network is not allowed unless the student has permission from a teacher or other school staff member.
e. Any file that is deemed inappropriate by school administration may be deleted from the schools computing resources without notice.

16) Access to School Databases

In some cases, students may receive general logins and/or passwords to school-acquired, academic resources in the internet. Students may not share logins or passwords for these resources with individuals outside of the school.

17) Online Subscriptions and Purchases

a. Students may not enter any other internet subscriptions, contracts or agreements while at school without the permission of a teacher.
b. Students may not provide personal information online in exchange for internet services.

C. Publishing Content Online

18) School Online Sites

a. Students may not upload content to the school's Internet site.
b. Students may upload content to the school’s intranet site.

19) Illegal Content

a. Posting pornographic, violent, racist, youth-inappropriate, or intentionally-harmful content on the school’s internet site or intranet site is forbidden.
b. Content should not be posted in the Internet or intranet that would bring harm to the school’s image.
c. Posting political or commercial advertisements on the school’s Internet or intranet sites is not allowed.

20) Copyrighted Content

a. Students may upload their own work to the school’s intranet site.
b. Students may not upload copyrighted digital media to the school’s

intranet site without the express, written permission of the copyright holder or copyright administrative organization and permission of a member of school staff.

c. Non-copyrighted material may be uploaded to the school's intranet site with the permission of a member of school staff. Non-copyrighted material includes public domain works, certain items under the creative commons license, and certain items under copyleft licenses.

d. Items that have been inappropriately uploaded to the school's intranet site or Internet site will be deleted as soon as they are discovered.

e. Students may not publish sites in the name of the school online without the express, written permission of the school administration. This is also valid for web addresses that are not hosted by the school itself.

21) Personal Photos

Students may not upload photos of other students, teachers or school staff members to the school Internet or intranet sites unless they have written permission from those individuals in the photographs. In the case that the photographed person is less than 18 years of age, written permission from that person's parent/guardian is required.

22) Social Networking

a. Students may not use the school's computer systems and network to access social networking, file sharing, instant messaging or chat sites in the internet.

23) Use of School Identity

a. Students may not enter into any Internet contracts or agreements on the behalf of the school without the express, written permission of the school administration.

b. Students may not publish content on behalf of the school on any Internet site without the express, written permission of the school administration.

D. Data Security

24) Supervisory Measures, Administration

a. The school has the responsibility to supervise student activity on the computer systems and the school network. For this reason, data and activities are monitored on the school's computer systems and network. Monitoring is done both manually through visual inspections and by electronic means.

b. IT administrators may freely access all files and folders stored on public, shared directories.

c. The IT administrators have the responsibility to protect users' privacy and will not distribute files stored in users' home directories to third parties except in cases outlined in clause 23b.

25) Email & Online Learning Tools

a. The school will provide accounts for email and online productivity tools for students.
b. School email and productivity tools should primarily be used for class purposes.
c. Students may not use the school computer systems, these accounts or the network for mass mailings or any other inappropriate messages.
d. Students must ask for permission from a teacher or school staff member before accessing their non-school email accounts.
e. Using another person's account is forbidden.

E. Additional Rules for the Use of Computers Outside of Class

25) Availability

a. School computers are not available for use by students outside of class time or the library without the supervision and permission of a staff member or teacher.
b. Neither school computers nor personal laptops may be used in the cafeteria.
c. During lunch periods, student laptops must be stored in students' lockers.
d. If a student is not in class, and the library is open, he or she should go to the library to use his or her laptop.

26) Supervisory Responsibility

Teachers and school staff members have the responsibility to watch and supervise students' use of school computing resources. Students must expect and allow such supervision.

F. Final Agreement

27) Parent/Guardian Signature

A student may not have access to the school's computer systems and network until this form has been signed by the student's parent/guardian and returned to the student's advisor. The returned form will be kept in school records.

28) Cases of Inappropriate Use

The school administration reserves the right to restrict the computer and/or network access of or temporarily remove the computer access from those students who do not adhere to the rules in the school. In serious cases, a student may be banned from the school's computer systems and network. Students who do not follow the rules outlined in this policy document may face additional disciplinary and/or legal (civil or criminal) consequences.

29) Appropriate versus Inappropriate Use

In individual cases, the school reserves the right to define further appropriate and inappropriate uses of the school's computing systems and network that are currently outside the scope of the current version of this document. Such a determination would be for actions that cause harm to the school, its students and/or its teachers or staff members. In the case that it has been determined that a student has acted inappropriately, and that student's actions do not fall within the terms of this policy, the school administration has the right to apply disciplinary actions as specified in clause 29. In some cases there may also be legal (civil or criminal) consequences.

30) Responsibility of the School

a. The school does not guarantee the function of computing resources in the school. Nor does it guarantee the modification of school systems to meet the individual demands of students.

b. Due to restricted resources, the school cannot ensure the backup of saved data on the school's computers or servers. Students have the responsibility to back up their own work.

c. The school administration has the right to alter this policy. In the case of a change, users will be informed in writing.

Dresden International School Computer and IT Use Policy

Please detach this form, sign it, and return it to the school. Students will be issued a login and password once they have returned this signed form to the school. Both the student and a parent/guardian must sign the document.

I have read and understood the policies set forth in the "Dresden International School Computer and IT Use Policy". By signing this document, I am accepting the terms set forth in the policy.

Student Name (please print):

____

____

____

Student Signature Location, Date

____

____

Parent/Guardian Signature Location, Date

[1]Information about Germany's *Jugendschutzgesetz* can be found at the internet site for the *Bundesministerium für Familie, Senioren, Frauen und Jugend* (http://www.bmfsfj.de). Translations of the law are available there in English as well as other languages.

"Jugendschutzgesetz." Internetredaktion des Bundesministeriums für Familie, Senioren, Frauen und Jugend,
6 June 2006. Bundesministeriums für Familie, Senioren, Frauen und Jugend.
<http://www.bmfsfj.de/Kategorien/gesetze,did=5350.html>. Last accessed: 17 August 2011.