INTERNATIONAL SCHOOL OF HAMBURG

IT Facilities and Services
ISH Secondary School Students

Purpose & Scope

The provision of IT facilities and services at the International School of Hamburg primarily serves to support student learning, academic research, professional development, and school administration in line with our educational mission. IT facilities and services includes but is not limited to: wireless or wired network access, software and cloud tools, desktop and portable devices, printers, scanners, projectors, storage media, and periphery. Access to these facilities and services requires users to understand their responsibility to use them in a responsible, safe, legal and ethical manner.

All Secondary Students are required to sign an agreement confirming they have read and understood this policy.

Responsibilities of Use

1. Use of IT facilities and services must be consistent with our educational mission
2. Do not let anyone know your password(s)
3. Use communication tools appropriately, ethically and respectfully
4. Respect the privacy and safety of others
5. Inform a teacher or staff member if you encounter inappropriate material on the internet
6. Respect copyright laws and ownership of works
7. Refrain from activity that may cause damage or otherwise jeopardize the security and integrity of the IT infrastructure

Detailed Description of Responsibilities

1 Use of IT facilities and services must be consistent with our educational mission

1.1 In order to comply with data protection laws and to maintain the value of your ISH work:

1.1.1 Do ISH work, only on ISH-managed platforms and

1.1.2 Do not send or store sensitive personal data or communications ISH should not have, on ISH-managed platforms.

1.1.3 Do not share sensitive information without authorization.

1.1.4 Do not put sensitive information in the subject line of emails or in the title of documents.

These are examples of metadata that is much more likely to be exposed in a number of scenarios: projector scenarios, over-the-back, tech trouble-shooting …

1.2 Do not use ISH online services (including the school network, email and G-Suite) to access, transmit, download or store media or communications not intended for educational purposes or related to school work.

1.3 Do not access, share, download or store material which is threatening, discriminatory, intimidating, abusive, harassing, offensive, pornographic, or obscene.

1.4 The network is a shared resource with limited bandwidth. Streaming multimedia or downloading/uploading large media files for private use is not acceptable.

1.5 Use of a mobile device (smart phone) when a class is in session needs to be agreed upon with your classroom teacher – it is otherwise not permitted.

2 Do not let anyone know your password(s)

2.1 Use strong passwords on school accounts. You are not only protecting your own digital profile and property, but often the digital profiles and property of others.

2.2 While knowledge of your username is required for sharing and communication, you should never let anyone (besides a parent or guardian) know your account passwords – even to "lend" your account to them temporarily.

2.3 If your username or account is used in an abusive or otherwise inappropriate manner, you may be held responsible.

2.4 Change your school password(s) immediately if you obtain knowledge or have suspicion that it is known by others.

3 Use communication tools appropriately, ethically and respectfully

3.1 All electronic communication using ISH online services, in particular, use of your school email or G Suite account should be responsible, respectful, safe, and kind.

3.1.1 Use academic and objective language: avoid using any language that might cause personal offense to the subject of your communication should he or she read it.

Be aware that under GDPR in some circumstances your emails may need to be handed over to the subject, if requested, unless good and valid reasons can be given not to do so.

3.1.2 Sending email, chat, video or voice messages that interfere with anyone's education or work at ISH is in violation of this policy and can attract severe disciplinary action.

Inappropriate use of communication tools includes sending messages that contain harassment, bullying, abuse, harassment, slander or threats, or messages that may offend a person on the basis of race, gender, sexual orientation or disability.

3.2 Forgery (or attempted forgery) of e-mail or chat messages is prohibited, as well as attempts to read, delete, copy or modify the messages of other users. This includes efforts to mask or hide your email or IP address.

Remember that electronic mail is not private. Think of e-mail or chat messages like an electronic "postcard".

3.3 Tampering with another user's school Google account and the digital property contained therein is strictly prohibited. If students are using shared devices and find that another user is still logged on to an account (Google, Veracross, or any online account) that user must be logged off immediately.

4 Respect the privacy and safety of others

Protection of individual privacy online is as important as sharing at ISH. Users are required to use the system in a manner that preserves the privacy and safety of themselves and others. German and European Data Protection laws also have strict stipulations governing the transmission of personal data.

4.1 Do not share personal information about individuals without their permission. This includes both text and numerical data about the person (biographical information, phone numbers, etc.), as well as representations of the person (graphical images, video segments, sound bites, etc.).

4.1.1 It is not appropriate to include a picture or video of someone on an internet page or social media site without that person's permission.

(Depending on the source of the information or image, there may also be copyright issues involved; cf. Policy 6).

4.1.2 Do not enter another student or teacher's email address or other information into a non-school managed website or service.

4.2 Do not use privileged personal information you obtained for a school-related or authorized purpose for a non-school-authorized purpose.

4.3 Do not try to access files and media of another user without clear authorisation from that user or without academic reason or authorization from the school.

Typically, this authorisation is given by setting file-sharing permissions to allow public or group access to files or media. However, errors can occur and such errors do not give users the right to access data they have no academic reason to access. If you are in doubt, ask the subject, the Tech Center, or School Administration.

4.4 Do not try to intercept or otherwise monitor any network communications not explicitly intended for you. These include logins, email, and any other network traffic.

4.5 Do not remotely access (log into) any workstation or device over the network unless you have explicit permission from the owner and the current user of that device.

5 Inform a teacher or staff member if you encounter inappropriate material on the internet

On a global network it is impossible to effectively control the content of data. Users when searching for educational material may inadvertently encounter inappropriate material, which the users, parents, teachers, administrators and other users around the device may find offensive or not academically appropriate. When such encounters mistakenly happen, immediately inform the supervising teacher or staff member and close the source of the material.

6 Respect copyright laws and ownership of works

6.1 Copyrighted materials are protected by law and subject to licenses and other contractual agreements. You must abide by these laws and agreements or risk being subject to civil or criminal prosecution. If you're unsure if you can use materials, please ask the IT department.

Some examples of illegal or limited use are:

6.1.1 copying and distributing software applications without license

6.1.2 downloading copyrighted music, movies and books using images, graphics and text without regard to the rights reserved by the owner, e.g. giving credit to the owner

6.1.3 using software or media for non-educational purposes (as per license agreement)

6.2 You should assume that all materials are copyrighted unless a disclaimer or waiver is explicitly provided. This is particularly true on the internet.

7 Refrain from activity that may cause damage or otherwise jeopardize the security and integrity of the IT infrastructure

7.1 Take all responsible care to prevent damage to devices and periphery

7.1.1 Do not attempt to remove or rearrange keys from a keyboard. This damages them permanently.

7.1.2 Report any damaged, missing, or rearranged keys to a teacher or staff member immediately

7.2 Avoid eating, drinking or placing liquid beverages in the vicinity of any computer system.

7.3 Do not re-configure computer systems or software or add/remove/disconnect accessories/software/services in any way that will inconvenience or confuse other users of shared devices or services.

7.4 Do not introduce malicious programs into the network (for example, computer viruses) or onto any device.

7.5 Do not attempt to repair any school owned electronic equipment. Please report the problem to the Tech Center.

7.6 If you believe the configuration of a workstation or device needs to be changed, please contact the TechCenter.

Violation of Responsible Use Policy

All ISH secondary school students are expected to follow this policy. Violations can subject the student to one or more of the following disciplinary actions:

1. A warning, followed by re-clarification of the Responsible Use Policy.
2. Notification of parents/guardians.
3. A (temporary) loss of device/network access privileges.
4. Suspension/expulsion.

Disciplinary action will normally be taken in the above order, but serious offences may lead to immediate loss of privileges and/or immediate suspension or expulsion.

If inappropriate use of technology occurs during the completion of class work, it can result in a failing grade for that assignment or class.