COLOGNE INTERNATIONAL SCHOOL
Internationale Friedensschule Köln

Cologne International School IT Acceptable Usage/ Safeguarding Procedures

January 2024 Revision for Parents and Students

CIS DIGITAL DEVICES: ACCEPTABLE USAGE POLICY

INTRODUCTION

Schools are constantly being challenged with regards to how computers and personal devices such as cell phones/smart phones/tablets can be used in constructive and educative ways, especially in classrooms and as part of the learning experience at school. At the same time, schools have to manage the use of these devices to avoid the possible risks that can be incurred from careless or malicious use.

The Information and Communication Technology (ICT's) infrastructure available at CIS is accessible to all members of the school community. Because the administrative staff, teaching staff and pupils are dependent on technology to do their work, it is imperative that there is consensus on how the equipment is to be used and what it is used for. Clear guidelines need to be given and a code of conduct established.

The policies and guidelines given in this document serve both to encourage and extend the use of electronic devices in constructive and educative ways as well as to limit and contain the possibilities of destructive or counter-productive instances.

Agreement to the conditions specified is a requirement for all who wish to make use of the technology available at the school.

This policy deals with:

SECTION 1: ACCEPTABLE USE POLICY FOR LAPTOPS AND OTHER MOBILE DEVICES

SECTION 2: NORMS OF BEHAVIOUR for ELECTRONIC COMMUNICATION and INTERNET USE

SECTION 3: MONITORING

SECTION 4: CONSEQUENCES OF BREACH OF THIS P0LICY

SECTION 5: ONLINE SAFETY

This policy is to be read in conjunction with the policies and principles that form part of the ethos and code of conduct of the school and are governed by the school's rules and regulations.

SECTION 1: LAPTOP ACCEPTABLE USE POLICY

GENERAL

The laptops have been introduced into the classrooms as a learning instrument, and their basic purpose is educational. Anything that enhances their educational potential is to be encouraged; anything that hinders them achieving their purpose is to be prevented. As they are educational school tools, the notion of privacy will be treated as secondary to the achievement of the school's educational purposes. Accordingly, if a teacher suspects that a child is using his machine for purposes other than educational during school time, that teacher will be entitled, and indeed expected, to intervene and inspect the contents of the machine to determine whether the facility has been or is being used for a purpose which is contrary to school policy. This would relate specifically, but not only, to the storage of illegal music files, pornography, antisocial material, hacking material or material that infringes copyright legislation.

IN CLASSROOMS

- Pupils should not listen to music while working without permission from the teacher.
- Pupils may not use E-mail facilities during class time unless instructed to by their teachers.
- Pupils should not display screensavers/backgrounds which are inappropriate or noisy.
- Pupils may not play games on their computers during class time unless the games are part of the teaching programme and have been required by the teacher as a class activity.
- Pupils should respect that the Internet is a shared resource and should therefore be circumspect and reasonable.
- Students must have all appropriate equipment to be able to participate in the learning activities. These include their technological device (laptop, not chromebooks), as well as exercise books, notebooks, pencils, pens, highlighters, erasers, sharpeners, etc.

PRINTING ON SCHOOL PRINTERS

The School does not provide access to school printers for students, so if printing in school is necessary, a request should be made to teachers in a polite and timely manner.

SECTION 2: OTHER TECH DEVICES (phones, smartphones, iPads, smartwatches, etc.)

Any personal information that can identify a person cannot be shared on any public forum without the permission of the person.

GENERAL

- Laptops are the main devices approved for learning, with an Apple and Microsoft system, by the school for personal use during school hours.
- Students can either bring their own personal device from grade 6 onwards, or they can rent it from the school free of charge.
- Students are expected to have their laptops **charged** every day.
- Pupils are permitted to have mobile devices (MDs) at school, however, they must be stored in their lockers. Any unauthorized use of MD will result in a detention and the device being confiscated and taken to the Principal.
- Using smartwatches for texting, calling, or any other purpose will result in them being taken away by teachers. They should always be stored in lockers from 8:05 until 3:30 or when lessons are over at the end of the day.
- Students should not expect to make or receive messages, calls, or any type of communication from parents or anyone else. If there is an emergency, parents can call the school or students can approach staff.
- If an MD rings during these times, the MD will be confiscated and taken to the Principal.
- The school accepts no responsibility for any loss of or damage to MDs, whether on campus or elsewhere. It is mandatory for students to store their MDs in a safe place at the beginning of the school day and until the end of the school day (8:05-3:30).
- Having any device during assessments risks disciplinary action.
- Headphones (airpods, earbuds, or any similar device) are not to be used during school hours unless specifically and explicitly instructed by the teacher. Headphones used in the mensa and lunch areas will be confiscated and will result in a disciplinary action.

ASSESSMENTS AND TECH. DEVICES

- Before tests or exams, pupils must hand in all any tech devices to the invigilators.
- MDs can be collected after the test/exam papers have been handed in at the end of the exam.
- Any student found in possession of an MD during a test or exam, even if inadvertently, may be charged with cheating and be disqualified and subject to disciplinary procedures.

SECTION 3: NORMS OF BEHAVIOUR for ELECTRONIC COMMUNICATION and INTERNET USE

ETHICAL PRACTICE

All members of the CIS community are expected to honor the school's values and practices. In doing so, they will not:

- bring the school into disrepute
- post any material on a website without the permission of the person or entity involved
- create a persona or digital ID on any social media site (e.g., Facebook, Twitter, Instagram, Tik Tok, etc.) which represents or pretends to represent the school without the approval of the Principal.
- Share pictures via email, WhatsApp, Instagram or any other social media platform.

THE CLASSROOM

- When teachers use or allow the use of the internet and/or social media for schoolwork, either in the classroom or as required work outside the classroom, participation in such online media is an extension of their classrooms in terms of what is permitted/acceptable online.
- Photographs may not be taken or videos or recordings made in a class without the permission of the teacher concerned.

LANGUAGE USE

- Messages posted publicly must not include any personal attacks.
- Messages should follow the rules of appropriate public language.
- Anytext transmitted to a public environment may not contain any language or content that the author would not be willing to share from the podium at a school meeting.
- Any work that shows disrespect of personal, political and/or spiritual values, and/or contains offensive remarks about race, gender, or religious beliefs.
- Inclusion of materials with excessive or gratuitous violence or explicit sexual content or activity that could be considered or perceived offensive by others

PORNOGRAPHY AT SCHOOL

Possession or distribution of pornography at school is considered to be serious misconduct as well as illegal, and will lead to exclusion from school. Viewing and/or circulating any material deemed by those in authority to be pornographic is a serious offense. As well as the above, activities that would be considered to be pornography include, but are not limited to: sexting, distributing naked 'selfies', distributing photographs/videos of a naked friend, distributing photos/videos of anyone involved in sexual activities.

BULLYING AND HARASSMENT

The following behavior is unacceptable at all times:

- Attacking CIS, the staff, the pupils or other people on any digital communication forum
- Cyber-bullying. According to the school's behavior policy, bullying includes but is not limited to:
    - behavior that can be construed to be the systematic, uninvited, repeated and intentional abuse of another person over a period of time
    - harming another person (hurting or embarrassing another person)
    - repeated threatening behavior which is intended to frighten another person
    - using electronic technology; for example, text messages or emails, rumors sent by email or posted on social networking sites, embarrassing pictures, videos, websites or fake profiles.
    - Insulting others
    - Using gestures or language directly or indirectly, literally or with irony, that alludes to race, ethnicity, nationality, gender, sexuality, religion, mental and physical health, disability, special educational needs or any other aspect of a person that renders them vulnerable.

PLAGIARISM AND ARTIFICIAL INTELLIGENCE

Plagiarism is the act of using someone else's work – words, images and ideas - without proper acknowledgement, and passing it off as one's own. This is fraudulent and is tantamount to stealing. Types of plagiarism include:

- Verbatim (word-for-word) copying, often achieved by using the 'copy-paste' function.
- Paraphrasing without acknowledgment: merely changing a few words in the chosen text.
- Using ideas generated by another person and presenting them as one's own.
- Submitting someone else's work or assignment as one's own.
- Giving one's work to another scholar to use as his own is also fraudulent, as one is complicit in the act of plagiarizing.
- Using any form of AI to produce work for school without permission of a teacher.

All information obtained during research from the internet must be referenced with the name of the site, the title and author of the article (if given) and the date accessed. Students may use APA, MLA or Harvard referencing.

THE INTERNET

Internet access enables pupils to explore thousands of libraries, databases, museums and other repositories of information and to exchange personal communication with other Internet users around the world.

Families should, however, be aware that some material accessible via the Internet contains items that are illegal, defamatory or potentially offensive. The Internet is a large and unregulated global network and increasingly it is possible to find controversial material or behavior on the Internet that some may see as offensive or inappropriate. This includes pornographic material or material with explicit sexual content, and unacceptable behavior in private email or social networking websites.

While the intentions of the school are to use Internet resources for constructive educational goals, students may find ways to access other materials. We believe that the benefits to students in using the Internet in the form of information resources and opportunities for collaboration exceed the disadvantages.

Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. However, at school we are also involved in setting standards and in monitoring adherence to our rules and to the school's standards of behavior, and this involves teachers, IT staff, the principals, and board of directors.

As Internet facilities are a limited resource, users are expected to use them primarily for:

- direct educational purposes;
- accessing information for private interests or hobbies;
- constructive communication with other internet users, provided it is not anti-social in nature.

Users may not:

- Access material that is labeled as 'not intended for minors', even if they have turned 18.
- Download and make public or intentionally view any material that is pornographic, abusive or age restricted.
- Disseminate the addresses of any material that falls into one of the above categories.
- Students are **not allowed to use WhatsApp in school. It is the responsibility of the parents to make sure that their children are accessing age appropriate content and the legal requirements that class chats and WhatsApp entails. School is not responsible for any miscommunication or misconducts within these groups.**

EMAIL

CIS regards emails to be the same as paper messages. Therefore, any written communication should obey the correct rules of grammar, capitalisation and punctuation. Every student and parent gets a school email that should be used exclusively for academic purposes.

Users must accept the privacy of email messages; mail may not be read by another person and care must be exercised when forwarding messages to ensure that privacy is not compromised. Electronic mail may not be misused. The following are considered to be misuse:

- unacceptable language
- offensive messages
- mass mail
- hate mail
- junk mail
- sending or distributing games
- personal graphic images
- chain letters
- hoaxes
- anonymous mail
- age- restricted content
- distribution of viruses, hacks or cracks
- No email or attachment from an unknown source should be opened. These should be deleted.

SECTION 4: MONITORING

Students who break any of the above rules are subject to the normal disciplinary structures of the school. Please refer to the disciplinary rubrics in the behavior policy posted on the intranet.

Any policy additions will be communicated to parents or added to this contract and facilitated to parents by the school principals through the different channels of communication of the school (website, Managebac, online/face to face information evenings).

SECTION 5: ONLINE SAFETY

Managing the Internet

Internet activity within the school is closely monitored and filtered through the CIS Firewall and other support systems. Whenever any inappropriate uses are detected, the Systems Manager is notified and the incident is followed up with the Acceptable Usage Policy and Safeguarding Procedures.

CIS continuously supervises different apps that come with the Google Learning Spaces, sifting through appropriate apps for school use, and keeping in line with the German Data Protection Laws.

The school is in charge of reminding students that the school's digital devices and internet use has to be in line with the regulations that the school has put in place. They must also align with the curriculum of Online Safety, delivered throughout the different homerooms to

the students using different online tools, such as Common Sense Media, to teach students about online safety, data protection, understanding the consequences of uploading private information, discriminatory/racist online practices, abusive practices in the online world, and gaming. If Internet research is set for homework, staff will remind the students of their online safety training. Parents are encouraged to support and supervise any further research.

The internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. The school will:

- Regularly review the methods used to identify, assess and minimize online risks
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material
- Ensure, through online safety education and the school AUAs, that pupils know that the school's expectations regarding safe and appropriate behavior online apply whether the school's networks are used or not

Managing the School Email

The use of email within school is an essential means of communication for staff and students. Students at CIS currently do have access to school created, individual email accounts within school. Only these accounts should be used for any school related communications. Personal email accounts are not allowed for official school purposes for both students and staff.

Safer Use of Technology and Classroom Curriculum

1. Safe Use of Technology

At CIS, we offer a wide range of technology use. This includes access to computers and laptops, internet, which may include search engines and educational websites, learning platforms, cloud services and storage, email and messaging, access to different educational apps, access to new technologies through after school clubs, like robotics and AI, and access to a Maker Space in the Design Lab.

This means that teachers and the entire learning community constantly need to supervise and manage the access that students have to these learning tools, keeping in mind age appropriateness and legal aspects. All devices should be used in accordance with the school's AUPSPs Policy and with appropriate safety and security measures in place.

Members of staff should always thoroughly check websites, tools and apps for suitability before use in the classroom or recommending for use at home

Staff and pupils must consider copyright law and principles of academic integrity before using internet-derived materials (and where appropriate comply with license terms and/or acknowledge the source of information). Staff and students must comply with the IB's Academic Integrity policy, available in our school's Academic Integrity Policy.

2. Social Networking and Personal Publishing

Considering the continuous development of new apps, as well as the popularity of Social Media apps like Instagram, Snapchat, Twitter (X), Telegram, and TikTok, CIS is aware of the potential dangers that these might imply in our students' learning and online safety. CIS is aware that publishing personal information, or information about others, has become easier. This carries with it inherent dangers of data protection and therefore, social media use in school is strictly forbidden.

In addition:

· Consideration will be given, at all times, on how to educate students in their safe use.

· Students will be advised never to give out information that will identify themselves, their friends or their location.

· Students will be directed towards moderated sites.

· Students will be advised to use nicknames and avatars when using social networking sites in order to not give out sensitive or private information.

· Students will be encouraged not to publish photographic content of themselves.

· Students are not allowed to record videos or audios or lessons or life inside our school and post them on social media. This is a violation of school policies and has high consequences. It also goes against the protection of each child's data.

The school does not permit the students to access their private accounts on social or gaming networks at any time during the school day. It is the parent's responsibility to make sure that their children are using social media apps safely and that they are aware of their children's online footprint at all times, the apps that their children are allowed to access, and the content of their uploads to the internet.

3. Curriculum Content: Digital Citizenship

At CIS, Online Safety is taught as part of the homeroom curriculum. It is integrated into the units of inquiry in grades 1-5. Every year, students (from grade 6) have a designated unit towards online safety that includes the following subtopics taken from Common Sense Media resources:

1. Media Balance and Wellbeing
2. Privacy and Security
3. Digital Footprint and Identity
4. Relationships and Communication
5. Cyberbullying, Digital Drama & Hate Speech
6. News & Media Literacy

At CIS, teachers will be using both **NRW Media Pass and Common Sense Media** as a basic tool for teaching students about Digital Citizenship. We have chosen to use this resource library as it is curated for educational purposes and it develops a learning approach towards technology which aligns with our school's mission, vision and learning principles.

At CIS, we want to prepare students to live in a connected world and to feel empowered by their acquired technological knowledge. They must learn to navigate the online world and be agents of change and kindness in it. You can access **Common Sense Media Content** as a parent through the following link, and Media Pass through this link.

SECTION 5: CONSEQUENCES OF BREACH OF THIS P0LICY

The violation of school rules concerning the use of the network, electronic media and communication will result in the same disciplinary actions as would result from similar violations in other areas of CIS life.

Any breach of this policy will be dealt with according to the Behavior Policy of the school.