Information Technology (IT) Policy

Part I - Rules of Procedure for the Use of Information and Communication Technologies of Tallinn European School - Staff

1. GENERAL PRINCIPLES

1.1. **Aim and content:** the aim of the information and communication technology (hereinafter referred to as ICT) guide is to ensure the common understanding of the staff of Tallinn European School (hereinafter referred to as TES) of an appropriate and safe use of information and communication equipment. The acquisition and use of the equipment owned or rented by TES can take place only in accordance with the rules laid down in this guide.

1.2. Scope and responsibility

1.2.1. Updating this guide shall be the responsibility of TES' IT manager.

1.2.2. Compliance with this guide shall be monitored by the TES IT manager and TES.

1.2.3. This guide applies to all TES' employees and all other persons who use TES' ICT assets and/or information systems while participating in TES' work and include the services and resources of the computer network of TES and all ICT equipment and workstations (computer, laptop, terminal station, printers etc.)

1.2.4. The beneficiaries of the processes described in this guide are all employees of TES.

1.3. **The inputs and outputs of the process:** the process shall begin from signing of the employment contract and with starting to work at school of a new employee or an employee returning from a parental leave, or the emergence of a service request. The process shall end with the employee's leaving, or the service request being fulfilled. The output of the process is a smooth, accurate and secure use of the information system and its components.

2. DEFINITIONS

Device under the sole responsibility	a device, the use of which has been solely given to the user, in such a way, that the grant of use has been documented, and the user understands that s/he's acquired the possession and the sole use of the device (a mobile phone, a laptop, lendable devices)
TES	Tallinn European School with all its organizational units
Information system of TES	a set of interconnected information technology equipment (hardware, software) and data, which is used to collect, process, store, read and/or handle the information necessary for the performance of the tasks of TES
ICT	information and communication technologies
ICT assets	software, hardware (equipment, their parts and related items), documentation and other intangible assets the records of which are kept by the IT manager
Incident	an unplanned interruption of service, the degradation of quality or a component failure.
IT manager	an employee performing an IT manager's role at TES
Loss Event	damage, destruction, data leakage or loss of ICT assets (including data and small assets)
User	a pupil, an employee, a member of the management body or any other staff member of the TES who has been granted the right to use the information system
Lendable equipment	a device that can be lent from the IT staff in such a way that the borrowing period and the user borrowing the device will be documented.
Mobile data carriers	smartphones, handheld computers, tablets, flash drives, hard drives, flash memory cameras and video equipment, voice recorders and other information storage accessories
Modification	adding, upgrading or removing any component that impacts the services
Cloud	Microsoft Office 365 cloud environment provided by Telia and Microsoft, used by TES

3. GENERAL MANAGEMENT AND ORGANIZATION OF TES' INFORMATION SYSTEM

3.1. Co-operation between the IT manager and the user

3.1.1. The common goal of the IT manager and users is to comply with this guide in such a way as to avoid risks to ICT assets and information systems, while avoiding the violation of user privacy and disturbance of daily work.

3.1.2. The user shall consider that all the information that moves on the computer network of TES is traceable if necessary, and the security monitoring is carried out all the time, it is automated, and deviations will be logged. The user has the right to receive information about which personal data of theirs and how it is processed (including the data, both processed automatically and not automatically by TES' information systems, as well as data processed by the IT manager in other ways). For getting information, a written request shall be made to the IT manager/Director.

3.1.3. If there is a legitimate alert situation, IT manager shall have access to all TES' information systems and ICT assets for prompt clarification and elimination of the alarm situation and, if necessary, for restricting the use of the information system. The user shall perform all the requested actions to ensure access.

3.1.4. The user has an obligation to allow the IT manager to perform the operations necessary for maintenance, monitoring and inventory. If possible, the IT manager will consider user suggestions when determining maintenance times.

3.1.5. The IT manager shall inform the user if the privacy of the user is being compromised by the activity of the IT manager, or there is a suspicion that the user's privacy may be compromised, or if the user is expected to modify their routine workflows, or if any component or operating environment changes so that it will be noticeable to the user.

3.1.6. If the user has any complaints regarding the quality of the IT manager's work, he/ she should address directly to the IT manager. In case the solution is not found, the HR manager and the Director shall be contacted.

3.1.7. The user shall not refuse the operations necessary in the work process due to a need to identify themselves with an ID-card or information system-specific username and password. The user shall consider that such measures are necessary to ensure information security.

3.1.8. ICT assets may be removed from TES' premises only if authorized by this guide or if an authorization has been obtained under the procedure provided for in this guide.

3.1.9. The user shall not allow the use of any ICT assets by persons who have no rights to use the TES' information system.

3.1.10. The user shall use all ICT assets and resources in an optimal and sustainable manner and shall not interfere with the others using ICT assets and resources.

3.1.11. If a user or any other person in contractual relationship has any ICT assets during the employment relationship, s/he shall be obliged to return it to TES no later than on the day on which the employment relationship ends. No related asset shall be left on the personal record card of the document management system. The assets located at the user's workplace shall be left in their location. The assets exclusively used by the user or gone into the possession of the user in other ways shall be handed over to the IT manager (unless it is obliged by the contract or other regulations to hand the asset over to the Director).

3.1.12. Mass storage devices containing sensitive information like report cards, photos, exams, etc. which are no longer used, shall be physically destroyed. Defective or disposable data carriers, such as USB sticks, shall be brought to the IT manager to be destroyed.

4. REGULATIONS FOR ASSIGNING, CHANGING AND WITHDRAWAL OF USER RIGHTS

4.1. Principles for the management of the rights

4.1.1. As a rule, the assigning of user rights only takes place by user groups and the principle of the existence of a justified work-related need-to-know shall be followed.

4.1.2. The persons who have been assigned the user rights for TES' information system or its users have personal usernames and passwords for the use of the computer network and the information system.

4.1.3. The service requests related to changing of the rights shall be formulated in the writing and with justification.

4.2. Creating a User Account

4.2.1. TES HR manager shall inform the IT manager to create new user accounts (including the first name, last name, position, and access to e-mail groups).

4.2.2. The IT manager shall create a personal account for the user and forward the user the information needed to authenticate himself or herself before the first working day. A user account gives the user the right to use the network resources, the Internet, internal Web sites, Teams, and Office 365 license exclusively assigned to the user.

4.2.3. Upon the first logging in, the user shall immediately change the password pursuant to the article "Requirements for the password and its use" of this guide.

4.2.4. The use of special software or services must be requested from the IT manager directly.

4.3. Other rights

4.3.1. To add a user to a group of electronic mail, or to remove the user, the Deputy Director or the HR manager shall inform the IT manager.

4.4. Long vacations, illnesses, missions or other cessations of the employment relationship

4.4.1. If a user has a longer than a 90-day unplanned vacation, parental leave or pregnancy and parental leave or a work related trip or is away due to some other incapacity to work (e.g. illness) or if there are other bases for a refusal to fulfil work assignments (hereinafter referred to as the suspension of employment), during which the person's access to the information system of the institution is not justified, the employee's direct manager or the HR manager shall notify the IT manager at least two working days in advance, or if this is not possible, then at the first opportunity, before the suspension of employment of the employee of the

organizational unit. The notification shall contain the exact date of suspension of employment for the employee.

4.4.2. During the suspension of employment, the employee's user account and access rights to the information systems and the mailbox shall be kept unlocked only in cases where the employee's access to these resources is reasonably necessary during this period and the employee's direct manager has submitted to the IT manager a respective written justified request.

4.4.3. Before departing, the employee shall be obliged to put up out-of-office notifications on their mailboxes, which note the fact of leaving, and their substitute's contact information, if available.

4.4.4. The HR manager shall notify the IT manager of termination of the suspension of employment so that it would be possible to open a locked user account in due time. Upon the termination of the suspension of employment, the employee's rights and files shall be restored to the previous form, if his or her direct manager or human resources employee has not stated otherwise in the request.

4.4.5. If a user account has not been used for more than 90 days, the user account will be locked during the audit of user accounts once per year.

4.5. Changing of the rights and closing

4.5.1. The employee must give back any IT devices to IT manager on the last day of work.

4.5.2. After the termination of employment, the employee's mailbox shall be closed immediately or after a period indicated by the Director.

5. CODE OF PRACTICE FOR USING THE INFORMATION SYSTEM AND ICT ASSETS

5.1. Acquisition, installation, management and record-keeping of ICT assets

In TES, only IT manager shall deal with the installation, connecting with the information systems, configuration and management of ICT assets, (including software). The former also includes the modification or switching off firewall, antivirus, and other security features.

5.1.1. In the case of mobile data carriers, users can generally do the above-mentioned operations themselves, but in case of problems or if a user is not sure how to behave, the IT manager shall be contacted.

5.1.2. The IT manager shall manage and keeps records of ICT hardware and software.

5.1.3. ICT hardware shall be registered in writing in a format that can be reproduced. For the assets, the manufacturer, model, serial number and inventory number shall be recorded at the minimum. The inventory number shall be the manufacturer's unique identification number or the unique number issued by IT manager, the financial specialist.

5.1.4. The assets shall be marked on the acquisition in such a way as to enable a third party to understand that it is the property of TES.

5.2. Data storage in the information system

5.2.1. It is assumed that users do not keep any data that is not related to work in TES' information system and any data carriers included in the ICT assets. TES' information system (including E-mail) and ICT assets shall not be used for private communication or storage of personal files. However, if the employee still uses TES' information system and ICT assets to store non-work-related data, personal communication or to store personal files other forms of personal data (for example, personal correspondence via work e-mail, personal passwords stored in the browser, etc.), they will do so under their own responsibility and agree that TES IT may process the relevant data as follows: access the content of the data (except when the personal nature of the data is clear without reading the content), continuously track the data traffic security, create and maintain log files for data traffic, and delete data (i.e. the authority is not responsible for maintaining such data). The consent shall be deemed given if the employee confirms being familiar with this guide upon arrival to TES.

5.2.2. An exception from clause 5.2.1, shall be a mobile telephone, if it is given to a user as a device under their sole responsibility so that the user has a right to use it for personal communication. In this case, the employee shall be obliged to

remove all personal or otherwise non-work-related data from the mobile phone before returning it to the possession of TES and delete association of the mobile phone with his or her user account (Apple ID, Google ID, etc.). If the employee fails to do so, IT manager may delete the data from the mobile phone or request compensation for the equipment that has been rendered unusable.

5.2.3. Storing such data, files, software, etc. that are protected as an intellectual property of a third party and whose right of use is not available to the user or whose right of use the user is unable to prove in the TES' information system and on any data carriers regarded as the TES' ICT assets shall be strictly prohibited. It shall be also prohibited to store any data, files, software, etc. that are not in accordance with generally accepted moral standards or otherwise of a socially contradictory nature (i.e., any material that may damage the reputation of TES, if publicly disclosed) in TES' system of the agency and in the ICT assets of any medium. It shall be also prohibited to visit websites that allow viewing or using the content with the character described in this article.

5.3. Requirements for the password and its use

5.3.1. The password shall not contain the user account's name or user's full name more than to the extent of two consecutive characters.

5.3.2. The password shall be at least 8 characters long.

5.3.3. The password shall contain characters from at least three of the following categories:

5.3.3.1. English alphabet capital letters (A to Z),

5.3.3.2. English alphabet small letters (a to z)

5.3.3.3. Numbers (0 to 9),

5.3.3.4. Additional symbols (for example: !, $, #, %, õ, ä, ö, ü, Õ, Ä, Ö, Ü);

5.3.4. If a specific system does not automatically allow the verification of the conformity of a password to the requirements, the user shall ensure the conformity themselves.

5.3.5. The password shall be entered in such a way that any other person will not be able to monitor it.

5.3.6. A password shall not be derived from user information.

5.3.7. The password shall not be disclosed to anyone (including IT manager, the direct manager, etc.).

5.3.8. It is recommended to use different passwords in different information systems.

5.3.9. Passwords recorded in writing shall be kept encrypted or in a safe deposit box.

5.3.10. The password received when being assigned user rights is one-time, and the user shall be obliged to replace it by a new one when they first log in in the school network.

5.4. Use of computers

5.4.1. It shall be forbidden to install any software (licensed or unlicensed) on a computer without the consent of IT manager. It shall be prohibited to modify the standard computer settings, including hardware and software configurations, network addresses and other system parameters.

5.4.2. To maintain documents, the necessary files shall be stored in the TES' Office 365 cloud. The maintenance of documents in the computer's hard drive or external storage device shall be the responsibility of the user.

5.4.3. Upon leaving the computer, the computer shall be locked [Windows key + L].

5.4.4. A third person should not have the opportunity to use the computer.

5.4.5. Any activities that could damage the computer, shall be avoided. Upon being in doubt about the correctness of an action, the IT manager shall be contacted.

5.5. Use of equipment under the sole responsibility

5.5.1. Equipment under the sole responsibility have been registered to be in the specific user's possession and use. The use of devices (such as laptops, mobile phones, touchpads) under the sole responsibility of the TES' staff members may be authorized if this is necessary in the work process. In this case, the user shall consider that the device under the sole responsibility is under his or her responsibility

5.5.2. The transfer of the device and being in the possession of the user shall be documented by the IT manager.

5.5.3. The user shall hold the equipment under the sole responsibility, applying the same principles and at least with the same or greater care, than s/he maintains his or her personal devices of the same kind and shall ensure the preservation and maintenance of the devices.

5.5.4. The user shall exclude the use of the devices under their sole responsibility by unauthorized persons (including TES' staff members if the use of the device by them is not necessary in the work process) and shall keep the device at any time in such a place and in such a way as to ensure that the unauthorized persons do not have access to the device. A device under the standing sole responsibility may be taken out of TES' premises only if it is necessary for performing work. The user shall have a right to take the mobile phone under their sole responsibility out of TES' premises.

5.5.5. Devices under the sole responsibility shall not be left in an unattended place (e.g. a car, even if it is locked, into a training room, etc.). Devices under the sole responsibility may be left in one's own office on TES' premises, following the requirements stipulated in TES HR policy (locking rooms, computers and mobile phones, etc.). The user shall not permit any device under their sole responsibility to be used by persons unrelated to TES (including their family members). The user may leave the device under his or her sole responsibility in his or her dwelling, if all doors, windows and other entrances of the dwelling are locked.

5.6. Use of lendable devices

5.6.1. It is possible to temporarily borrow the following devices from the school: cables, cameras, laptops, iPads, external CD/DVD burners and video projectors (see more about video projectors in the Article 5.7). If one wants to borrow iPads or laptops, they must be booked beforehand via Sharepoint (Tallinn European School/16 - iPad & Laptop Reservation). For any other devices, the IT manager needs to be contacted directly.

5.6.2. The borrowed device must be used either for teaching in class, a class or

5.6.3. pupil project, teacher's lesson preparation or any other work related activity in fulfilling the duties in TES. Private use is prohibited.

5.6.4. The borrowed device shall be returned in the same upkeep, as it was and not later than the end time of the booking.

5.7. Use of video projectors

5.7.1. Upon using a projector on the TES' premises, the projector shall be normally installed by a handyman. The user shall connect the projector to the computer, turns on/off the projector display mode and provide that the projector would not work being unused for more than 15 minutes. There is a special on/off button on the control panel of the projector to switch the display mode on/off. It shall be forbidden to interrupt the supply voltage of the running projector by a switch, or pulling out the power cord, because it threatens the projector lamp and control electronics.

5.7.2. In the case of a request to use a lendable video projector outside of TES, the user shall approach the IT manager about receiving respective instruction (if he or she has no such previous experience or skills).

5.8. Use of video conference equipment

5.8.1. As a rule, Teams and built-in camera and microphone of a laptop are used for video conferences.

5.8.2. If the user wishes to use video conference equipment independently, they shall approach the IT manager for instruction, if they have no previous related experience or skills.

5.8.3. At the end of the use of video conference equipment the user shall turn off the devices in the room.

6. CODE OF CONDUCT FOR SERVICE REQUESTS AND INCIDENTS

6.1. User support

6.1.1. In the event of service requests or incidents, the user shall approach:

6.1.2. The IT manager.

6.1.3. The user support function shall be performed by the IT manager.

6.1.4. The IT manager shall have a right to determine the ultimate priority.

7. CODE OF CONDUCT IN THE CASE OF LOSS EVENTS

7.1. Loss events involving theft of the device not under the sole responsibility

7.1.1. If the user is unable to prevent the loss event or reduce the consequences thereof, they shall immediately take respective measures.

7.1.2. If the user becomes aware of any loss event, or suspects that there has been a loss event, they shall notify the IT manager immediately (no later than during the same working day). If possible, the user shall do it in the form, which allows reproduction (e.g., e-mail). Express notification is important, because the asset may be insured, in which case the time limit for the notification of the insurance case must be followed. In addition, express notification is important to enable the IT manager, if necessary, to shut down access to the institution's information system through the device and thus avoid further damage.

7.1.3. The user shall provide the IT manager with as much information about the incident as possible. The user shall pay attention, inter alia, to the fact whether the incident may have been caused by a TES staff member with their intentional or careless conduct.

7.1.4. If there is evidence that the user has caused the loss event due to intentional or careless behaviour, the user shall be liable for damage to the extent provided by law. In this case, the determination of the size of the damage and liability, the assessment of the evidence and making the respective decision shall take place in the cooperation of the IT manager and the TES management. Settling loss events shall be based on the same procedure than in the case of loss events with assets under the sole responsibility, but the IT manager, in co-operation with the TES management, may, at its own discretion, decide on the simplification of the procedure in each specific case if that is reasonable.

7.2. Loss events involving assets under the sole responsibility

7.2.1. If the user can prevent the loss event or reduce the consequences thereof, they shall immediately take respective measures.

7.2.2. In the event of damage, destruction, or loss of a device under the sole responsibility, or in the event of respective doubt, the user on whose behalf the device is/was registered shall promptly submit the primary notification of the loss event or suspicion thereof. The explanatory statement shall be sent either to the IT manager's registered e-mail address. The explanatory statement must include at least the following: the date, the user's name, the device data, a description of the event as detailed as possible, and the user's proposal to resolve the situation.

7.2.3. Upon receipt of an explanatory letter, the IT manager shall decide within 5 working days whether the loss event is deemed to be closed (i.e., no claim will be filed against the user and the case will not be processed) or the resolution of the loss event shall be decided in cooperation with the TES management. The IT manager may independently close the case if the set of circumstances of the case justify this, for example, if it is clear that the evidence is inadequate and the damage is not great, or if it is clear that the loss is low (less than 50 euros) or if it is seen that the user's fault is very small (the user can only be considered neglectful to a very small extent). In both cases, the IT manager shall inform the user and the TES management about the decision in writing.

7.2.4. In case the IT manager cannot independently consider the case closed, he/she shall, in cooperation with the TES management, evaluate the following:

7.2.4.1. the extent of loss;

7.2.4.2. level of culpability (negligence, gross negligence, intent), taking into account all relevant circumstances, in particular the user's duties, instructions given to the user, working conditions, the normal risk arising from the nature of the work, user's training, user's professional knowledge (including the requirements set for their position), the duration of working at TES and the behaviour to this day, the capabilities and characteristics of the user that TES knew or had to know as an employer;

7.2.4.3. the extent of liability (i.e., if the amount of damage has been determined, to which extent the user should be responsible for), taking into account all the relevant circumstances, in particular the level of culpability (in the event of intent, the user shall be liable for all the damage), the user's remuneration, as well as the TES' reasonably presumable ability to avoid or insure against damage, and to what extent the damage was caused by the realization of the risk of a typical loss associated with the activities of TES.

7.2.5. The IT manager, together with the TES management, shall decide on the loss event. If it is decided to claim damages from the user, the claim together with the decision shall be submitted in a written notice addressed to the user. If the user's negligence is detected and the user is required to pay all or part of the loss, the decision shall reflect how the consideration process was carried out (which factors were considered and what were the reasons for determining the amount of damages claimed).

7.2.6. If the user does not agree with the decision, he/she can submit respective objections to the TES management. The objections shall be submitted in a written

and signed form, accompanied, where appropriate, by evidence. The objections can be filed within 30 calendar days from the date of receipt of the decision (for the period of a leave, mission, other legal absence or sick leave, the time limit shall be suspended). The objections shall be deemed filed if they have been forwarded to the e-mail of at least one member of the TES management. In addition to the statement of reasons the objections shall include a clear request, especially whether the user does not agree or agree only partially agree with the required damages. The TES management shall decide on the acceptance or non-acceptance of the objections within 10 working days. If the objections need to be clarified, the TES management may extend the deadline. If the user still does not agree with the decision, he/she may contact the labour dispute body.

7.2.7. If the TES management has decided and sent the user a claim for compensation, and the user has not objected to it within the set deadline, the user shall compensate for the damage. If the decision does not provide for a different term and the parties do not agree otherwise, the damage shall be compensated no later than within 60 calendar days after the receipt of the final decision. Upon request, a user may file an application for the compensation to be deducted from their salary (otherwise the damage will be compensated by a separate payment). The user may unilaterally determine that the damage will be deducted from his or her salary over a longer period, broken down monthly, but in this case, one part may not be less than EUR 25.

8. NETIQUETTE

The following paragraphs introduce the TES email etiquette and guidelines to ensure professional and safe electronic communication.

8.1. General Guidelines

8.1.1. The main communication tool at TES is email.

8.1.2. TES staff uses exclusively TES email (firstname.lastname@est.edu.ee) for any communication within TES and with contacts from outside TES. This includes emails to: TES staff, pupils, parents and third parties related to work at TES.

8.1.3. TES staff uses TES email for signing up to third party services, like, Khan Academy or any other thirds party service related to work at TES.

8.1.4. For quick informal communication within TES, Teams is recommended.

8.1.5. The TES values: Respect, Harmony and Creativity, are also the core principals regarding the use of TES' IT devices and digital communication with others within and outside of TES.

8.1.6. Parent-teacher communication at TES should be handled via announcements in MySchool or via email, e.g., indication of a pupil's absence by parents.

8.1.7. It is advised to read and send emails and other messages only during working hours.

8.2. Email Etiquette

8.2.1. Use the "reply all" option only in justified cases.

8.2.2. Maintain privacy. If you send an email to a list/group of people that do not know each other, use the "Bcc" field, e.g., ask parents if they agree on sharing their email.

8.2.3. Include a clear subject line. Choose one that lets readers know you are addressing their concerns.

8.2.4. Use professional salutation. "Dear (and the name of the recipient)" is preferred.

8.2.5. Mind content and language. Be polite.

8.2.6. Avoid humour or irony as it can be easily misunderstood.

8.2.7. Abbreviations, emoticons, jargon, or slang is not appropriate.

8.2.8. Use exclamation points sparingly.

8.2.9. Never use upper case letters only as it is regarded as yelling.

8.2.10. Refrain from sending one-liners. Feel free to put "No Reply Necessary" at the top of the email when you don't anticipate a response and/or use Teams.

8.2.11. Only discuss public matters. Anything in the digital domain can be copied and can become public.

8.2.12. Sending confidential information should be avoided for security reasons.

8.2.13. Respond in a timely fashion.

8.2.14. Emails must include a “Signature Block”. TES signature block must contain: first name, last name, position, email address, the official TES logo and TES Address provided by Communication manager.

8.2.15. Avoid large or multiple attachments. Use link sharing instead and set the permissions.

8.2.16. accordingly. For working group documents, use Teams, OneDrive or Sharepoint.

8.2.17. Proofread your email before sending it.

8.3. Cyber-Security

8.3.1. TES staff is obliged to follow the general cyber-security principles.

8.3.2. Password Security: Passwords must be at least 8 characters long and contain lower case and uppercase letters and numbers. Do not use the TES IT standard password. Do not use predictable passwords. Do not use the same password for different services, e.g. do not use the same password in TES and in MySchool. Do not share passwords with others.

8.3.3. Turn to IT manager in case you forgot your TES password, or you think somebody else might know it.

8.3.4. Delete suspicious emails without opening them.

8.3.5. Check the sender and the email content before opening an attachment.

8.3.6. TES IT manager will never ask you for your credentials (or any other confidential IT information) over phone or via email.

8.3.7. Antivirus software must be updated regularly.

8.3.8. Protect sensitive information. Only store confidential or sensitive data of colleagues, pupils or parents if necessary.

8.3.9. Store important data in several secure places. At least on your laptop and backup to OneDrive.

8.3.10. TES staff is self-responsible to back up their data.

8.3.11. Avoid using mobile storage like SD cards, USB sticks.

8.3.12. Do not use mobile storage from people outside TES.

8.3.13. All used devices must be password protected.

8.3.14. Avoid using public/unsecured Wi-Fi outside TES with your work device.

8.3.15. If you leave a device unattended, you must lock the device before you leave.

8.3.16. Do not share any information from work in social media like Facebook, Twitter and alike.

8.3.17. Apply maximum privacy settings on social media accounts.

8.3.18. Installing software on TES' IT devices is exclusively done by the IT manager.

8.3.19. Avoid downloading files from websites.

8.3.20. Report a lost or stolen device immediately.

Part II - Rules of Procedure for the Use of Information and Communication Technologies of Tallinn European School – Pupils

1. GENERAL PRINCIPLES

1.1. This policy was researched and compiled by the IT manager and educational technologist of TES, supported by management, administration, teachers, and pupils. The aims of this policy are to:

1.2. Ensure that pupils benefit from all learning opportunities offered by the computing and internet resources provided by the school in a safe and controlled manner.

1.3. Ensure that pupils benefit from the use of their own IT devices in the school environment.

1.4. Give pupils clear guidance on safe and acceptable use of these resources (Annex 1:

1.5. TES Microsoft Teams Netiquette).

1.6. Make pupils aware that internet use in school and the school's Wi-Fi are resources. If the resources are abused, then access will be denied.

Furthermore:

1.7. TES teachers may prohibit all use of interfering and electronic communication devices during instructional time. Instructional time includes class time, assemblies, and field trips. Schools may prohibit the use from the first lesson until the end of the final lesson, including class breaks, recess, and lunchtime.

1.8. TES teachers may allow specific devices for curricular purposes only. Teachers may not allow interfering or electronic communication devices as part of a "reward" or "free time."

1.9. Any member of staff has the right to confiscate personal mobile phone, smartphones or other ICT devices that will be handed over to the Deputy Director(s) or the Educational Adviser. The devices will be confiscated until the next morning for the day if the pupil has been caught using it for their personal use in the very end of their school day. The items will be kept in respective offices and can be collected at the end of the school day. The parents will be informed of the event by e-mail.

1.10. Cell phones, cameras, and any device which can compromise personal privacy, such as in a locker room and/or bathroom are prohibited. The violation of one's privacy in such a manner will result in consequences, including TES disciplinary council and a law enforcement referral.

1.11. Any device used in a way that might reasonably create an impression of being threatened, humiliated, harassed, embarrassed, or intimidated is prohibited. Any use in this manner will result in consequences, and possibly a law enforcement referral.

1.12. Smartphones, smartwatches, laptops, or any device used for cheating during tests and exams will result in a hearing of the TES disciplinary council.

1.13. Photographing, recording, or filming on school premises is allowed only with the permission of the teacher while using it for learning purposes. Same holds for uploading this content to the internet and social media.

1.14. Photographing, recording, or filming pupils, teachers, or other staff members and/or uploading this content to the internet and social media is strictly prohibited. It can be only allowed after all parties involved gave their explicit consent.

1.15. Designated areas for use of ICT devices are the library, Mont Blanc Lounge, Front office, Study Room and classrooms if agreed with the class or subject teacher.

2. USE OF SCHOOL'S ICT DEVICES IN LESSONS

2.1. TES IT manager provides ICT devices (tablets or laptops), which must be booked using the booking system.

2.2. ICT devices must be booked, picked up and returned in time, to ensure a failure-free operation.

2.3. ICT devices are for teaching purposes only.

2.4. ICT devices can be used only on the school's premises and not be taken home by pupils, teachers, or other staff. Exceptions, e.g., for SEN pupils and for distance learning periods must be discussed and agreed individually with the IT manager.

2.5. ICT devices must be handled carefully.

2.6. Teachers are expected to guide pupils using ICT devices.

2.7. Any damage must be reported immediately to IT manager.

2.8. The violation of the regulations set out in this paragraph will result in the temporary or even permanent exclusion from using TES ICT devices.

3. USE OF SCHOOL'S ICT DEVICES OUTSIDE LESSONS

3.1. TES IT manager also provides ICT devices Library computers for use outside of lessons e.g., during free hours or breaks.

3.2. ICT devices are for learning purposes only.

3.3. ICT devices are provided in the library.

3.4. In exceptional cases, ICT devices can be borrowed using IT lending system, after discussing individually with the IT manager.

3.5. ICT devices can be used only on the school's premises and not be taken home by pupils, teachers, or other staff.

3.6. Pupils using those devices on their own must have experience in using them.

3.7. Pupils can use ICT devices in designated areas only.

3.8. Pupils can use ICT devices under the supervision of a TES employee.

4. USE OF PERSONAL ICT DEVICES IN SCHOOL

4.1. ICT devices are tablets, laptops or any other physical hardware or equipment that provides one or more computing functions within a computer system.

4.2. Pupil's personal ICT devices can be used in school for learning purposes only in accordance with the BYOD policy (**Error! Reference source not found.**).

4.3. The use must be agreed by the class or subject teacher.

4.4. Only Secondary pupils are allowed to use their personal ICT devices independently for learning purposes, in designated areas only.

5. USE OF SMARTPHONES IN SCHOOL

5.1. The use of smartphones on TES premises (inside and outside) for pupils is strictly prohibited for personal use.

5.2. Teachers must enforce the prohibition of smartphones on the premises at any point.

5.3. In case a pupil violates these rules, teachers are encouraged to confiscate the pupil's smartphone immediately.

5.4. Pupil's confiscated smartphones will be taken to the deputy director of the pupil's school level and stored there for the day and can be picked up by the pupil after school.

5.5. The only exception is the explicit use of smartphones in class for teaching purposes. In this case, teachers facilitate the correct smartphone use in the lesson.

5.6. Teachers and staff should not use their smartphones publicly in school to set a good example for pupils.

5.7. Teachers and staff should encourage parents and guests to use their smartphones in designated areas only to set a good example for pupils.

Annex 1:

TES Microsoft Teams Netiquette

Microsoft Teams Netiquette

Sound Use in 10 Steps

1 #Respect
I am kind and polite in Teams just as in real life.

2 #Camera
I join the video call with my camera on. I do not record or take screenshots during video calls.

3 #Writing
I use good spelling, capital letters, punctuation and no abbreviations.

4 #Directions
I follow my teacher's directions about turning my video and microphone on and off.

5 #Privacy
I don't post anyone's private information (photos, phone numbers, addresses).

6 #Ownership
When I share something, I indicate its origin (author, link...).

7 #Cooperation
I work nicely with others, use positive language and avoid criticizing others.

8 #Chat
I only use the meeting chat during a video call to comment on the lesson activities, not to chat with my classmates.

9 #Focusing
I close all other programs and games so I can focus properly during the video lesson.

10 #Safety
If I have a problem with someone on Teams, I tell my parents or my teacher.

#Commitment: I'm looking forward to doing awesome schoolwork with Teams. I share my ideas and what I can do. I help others and I try to amaze everyone.

Annex 2:

Bring Your Own Device (BYOD) policy

FOREWORD

Tallinn European School (TES) strives to offer its pupils the best conditions for learning and working with digital equipment. To support this effort, the strategy calls for permitting pupils to use personal devices (of their own and of their choice) for school-related activities by connecting them to the TES network.

Pursuing this educational goal requires adopting a “Bring-Your-Own-Device Policy” (hereafter “BYODP”) to clarify what may or may not be considered as an acceptable use. The present BYODP outlines the rules for the proper use of personal devices from an ethical and legal point of view. It is also meant to protect the security and integrity of the TES data and technology infrastructure.

This policy constitutes an annex to TES IT policy and is part of the binding regulatory framework to which students are subject. For it, the term "device" refers to a mobile digital device (tablet or laptop computer) that can be connected to TES Wi-Fi network.

ACCESS TO TES NETWORK

Pupils may access TES network for pedagogical purposes only. It entails having access to:

- both shared and personal data storage on OneDrive.

- Office365 (including the e-mail service) managed by TES.

- MySchool – School Management Software;

- proprietary or open-source software;

- TES password protected Wi-Fi network.

Accessing TES network is a privilege, not a right. TES reserves the right to revoke this privilege if pupils do not abide by the rules outlined in the present policy.

Access credentials are provided by the IT Manager and sent to the guardian emails provided to the school upon arrival.

CONFIDENTIALITY

Access to network accounts is personal and individual and may not be shared.

Access credentials are confidential, and may not be divulged to third parties, except for the pupil’s legal representatives. Pupils must report any problem they would encounter with their account to the IT Manager or in their absence the Educational Technologist.

As regards confidentiality, the following will be considered as a breach of the present policy (it being understood that the list is not exhaustive):

- trying to find out another person's password;

- logging in with another person's username and password;

- opening, editing, or deleting the files belonging to another person and/or generally trying to access another person's account.

ACCEPTABLE USE POLICY

Each pupil is personally responsible for his/her actions in accessing and using a device on TES network. Failure to comply with the rules for acceptable use will result in disciplinary action, which may also include suspension of computer privileges, resulting in a failing grade for work requiring the device in class.

TES defines acceptable use of personal devices as school-related activities in connection with the mission of the European Schools. Pupils are blocked from accessing certain websites[1] during school hours/while connected to TES network at the discretion of TES and are not authorized to connect to chat services, discussion forums, or social networks without the express permission of a member of the educational staff.

Devices may not be used at any time to illegal or harmful purposes.

The following list, though not covering every situation, specifies some of the conduct that violates the acceptable use of the device:

- intentional damage to hardware or software, or the creation or distribution of viruses, worms or other forms of digital mayhem;

- creating, displaying or transmitting threatening, racist, sexist, pornographic, negationist, abusive or harassing language or materials;

- storing or transmitting illicit materials;

- unauthorized use of a computer account or distribution of a password;

- plagiarism or intruding into other people's files;

- using electronic mail to harass or threaten others, including sending repeated, unwanted e-mails to another user. This is in line with the school's anti-bullying policy;

- using e-mail lists or personal information for purposes other than those that are pedagogical or educational in nature;

- giving your name, address, or phone number to anyone over the Internet[2];

- downloading and/or installing any software including, but not limited to, executable files, games, MP3 files or players, video files, zip files, where these are not authorized by a teacher;

- viewing a website which was not approved by your teacher or viewing a website not in line with instructions for your work during class.

[1] Forbidden websites include, but are not limited to social media webpages, age restricted websites. The following apps are not allowed: social media applications.
[2] Under no circumstances should the pupil give out his/her full name, photo, address, telephone number, or any other indicator facilitating his/her identification on the Internet.

Within the framework of the BYOD policy **devices may be used by S4-S7 pupils** in the following areas for learning purposes only:

- Library
- Study room
- Mont Blanc Lounge
- La Grande-Place – Second floor lounge area (B-building).
- In the classrooms with the permission of the teacher

DEVICES AND SUPPORT

Smartphones (multifunction mobile phones) are allowed only for educational purposes in class and under the supervision of a member of the educational team. Their use is limited due to the small screen size.

Tablets are allowed.

Laptops are allowed. Chromebooks are not advised.

Connectivity issues will be supported by the IT Manager.

Devices' camera and/or video capabilities must be disabled while on-site, except in the case of a request from teachers in the pedagogical framework.

SECURITY

In order to prevent unauthorized access, devices must be password protected using the features of the device. A strong password is provided to access TES network according to the IT policy.

As regards security, the following is strictly prohibited policy (NB! the list is not exhaustive):

- installing software or making a copy of software present on the network;

- deliberately disrupting network operation, including the use of programs to circumvent security or introduce malware (viruses, spyware or others);

- diverting or attempt to bypass protection systems in place (firewalls, antivirus…);

- using VPN.

RISKS AND LIABILITIES

Pupils maintain complete responsibility for their device. As stipulated in Article 34 of the General Rules of the European Schools: "The school shall not be responsible for objects brought to school by pupils".

We strongly recommend purchasing device insurance.

While TES will take every precaution to prevent the pupil's personal data from being lost, it is the pupil's responsibility to take additional precautions, such as backing up email, contacts, etc.

TES reserves the right to disconnect devices or disable services without notification.

Lost or stolen devices must be reported to TES within 24 hours. Pupils are responsible for notifying their mobile carrier immediately upon loss of a device.

Pupils are liable for all costs associated with their device.

Pupils assume full liability for risks including, but not limited to, the partial or complete loss of personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

TES reserves the right to take appropriate disciplinary action up to and including a definitive exclusion for noncompliance with this policy.

PENALTIES

Any student who violates the present policy will be subject to disciplinary proceedings as per the General Rules of the European Schools and TES School rules, as well as penalties and criminal proceedings prescribed by law. Teaching staff will exercise strict control in order to ensure respect of the rules by the pupils they are responsible for.

The network administrator must ensure the proper working order and use of TES technology infrastructure. To this end, the monitoring makes it possible to detect anomalies (excessive use of the network, excessive storage space, attempted cyber-attack, etc.).

In the event anomalies are detected, the IT Manager will ask TES management to agree on the measures to be taken. But in case of absolute urgency, and to protect TES computer system, the IT Manager may make the decision to immediately block accounts for one or more pupils, then immediately inform the management.

This type of intervention can only be carried out for clearly defined purposes, namely:

- the prevention of unlawful or defamatory acts, acts contrary to morality, or likely to undermine the dignity of others;

- the protection of the confidential, economic, or financial interests of schools, as well as the fight against those responsible for attempting any such unwarranted access;

- the security and/or proper working order of the IT systems, including the control of related costs, as well - as the physical protection of the school's facilities;

- ensuring respect for the principles and rules regarding the good faith use of available technologies.

PROTECTION OF PERSONAL DATA

TES undertakes to process personal data collected in connection with the use of personal devices in strict compliance with the General Data Protection Regulation.

SIGNATURE

The signature of this policy is mandatory for any pupil willing to connect a personal device to TES network.

Name:

Class:

Signature:

ANNEX 3:

Official guidelines for choosing a mobile device related to the BYOD Project

Based on the "Guidelines for the pedagogical use of mobile devices in the European Schools" (Ref. 2020-01-D-14-en-2)

The choice of mobile devices is an essential point in the digital equipment of institutions and schools. Indeed, mobile equipment often comes with an ecosystem in which it is integrated: hardware management tool, software management tool, application acquisition process, information security and personal data protection. The hardware support and the different stages of preparation of a mobile device are also important points in the choice of equipment and associated services.

The guidelines are intended for stakeholders involved in acquiring of mobile devices who will find recommendations to guide them in their choice.

The requirement levels in the recommendations are expressed using specific words, based on the RFC 2119[3] terminology:

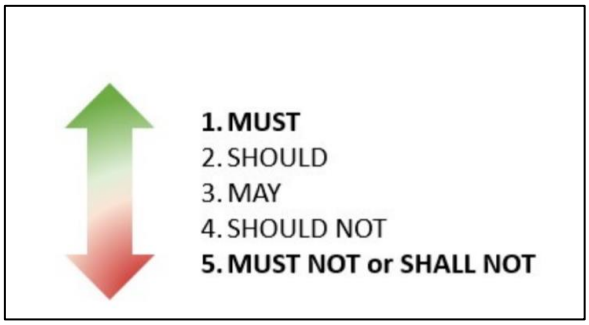

Table 1: Signification of the level of recommendation:

MUST	the element is an absolute requirement of the specification.
SHOULD	there may be valid reasons in particular circumstances for ignoring a particular element, but all implications must be understood and carefully weighed before choosing a different path.
MAY	the element is truly optional.
SHOULD NOT	there may be valid reasons in particular circumstances where a specific behaviour is acceptable or even useful, but all implications should be understood, and the case carefully weighed before implementing any behaviour described withthis notation.
MUST NOT	the element is an absolute prohibition of the specification.

[3] https://www.ietf.org/ The Internet Engineering Task Force (IETF) is an open standards organization, which develops and promotes voluntary Internet standards; Requests for comments (RFCs) are a numbered series of documents published by the IETF and describing the technical aspects and specifications of the Internet, or of different computer hardware.

1. Hardware features

Feature	Recommendation for mobile device	Reason
Screen size	SHOULD be greater than 9 but to a maximum of 14 inches	A size smaller than 9 inches penalizes the possibilities of reading and producing content. A screen size bigger than 14 inches might be too big for the schoolbag and the table during lessons.
Resolution	SHOULD be min 1080p	To display documents, graphs, tables, and text properly and to work on the device the resolution should be 1080p (FHD) or more. 720p (HD) is possible, but for proper work in Office, it is too less.
Weight	SHOULD NOT exceed 1.2 kg excluding accessories	For the same reasons as above.
Connectivity	MUST have Wi-Fi, Bluetooth (minimum 3.0)	Students and teachers need to connect to the internet via the school's network and to wireless accessories (headphones, mouse…).
Screen cast	SHOULD be able to wirelessly connect to a beamer or screen.	This encourages the sharing of students' work in the classroom and collaborative work.
Battery life	SHOULD offer sufficient battery life for one school day.	The classrooms are not equipped to load all the students' mobile equipment. Note that during a normal school day, the device is not necessarily permanently switched on. In case of a smaller device (< 10 inches) 30 Wh and in case of a bigger device 50 Wh are good.
Storage	Available memory SHOULD be at least 32 GB and SHOULD be a Flash Memory (SSD, EMMC…) MAY be equipped with an external memory.	The mobile device also MAY be equipped with an external memory such as a micro-SD card to expand its memory capacity. A spinning hard drive (HDD) is not so durable in a mobile device.
RAM	Tablets (Android, IOS) SHOULD have at least 2 GB of RAM. Laptops or convertibles (Windows, Linux, MAC OS, Chrome OS) MUST have at least 4GB	The device gets very slow when the RAM is fully used by the OS and the applications. For proper work enough RAM is very important.
Camera	SHOULD have at least one camera	In order to make photos of documents or students' work and make small videos for learning reasons. The quality of the camera SHOULD be adapted to the use.

2. Accessories

Feature	Recommendation for mobile device	Reason
Protection	Protective cover or shell SHOULD be associated with the MD (if it is not reinforced to limit damage).	To sustain the lifetime the device SHOULD be protected in some way to avoid damages on screen and device. The protective cover SHOULD allow the mobile device to be placed upright or tilted, not just flat, making it easier to view the media.
Keyboard	A physical keyboard SHOULD be associated with the MD	Tablets all have virtual keyboards, which are not suitable for mass content production, especially in Secondary. Thus, a physical keyboard compatible with the mobile equipment SHOULD be associated with the mobile equipment. However, the virtual keyboard has the advantage of being able to adapt to the context of the use of the device (e.g., various languages) and offers a solution to the problem of specific characters.
Accessories	MAY be associated with the mobile device, but MUST be adapted so as not to interfere with its use	Mobile equipment must be able to respond to many situations and allow a variety of uses. Accessories MAY be associated with the mobile device (e.g., pointing pen, fine-tip stylus for writing with the hand, technical probes, etc.), depending on the educational uses expected in the school or establishment, or special needs (e.g., disability compensation). Several subjects or situations (modern languages, music education, school outings, podcasting, certain cases of visual impairment) require the use of headphones or earphones. The accessories selected to complement the mobile equipment MUST be adapted so as not to degrade its use. For example, make sure that the protective cover does not obstruct the camera, microphone, speakers, plugs, buttons...