

Pravidla informační bezpečnosti

Regulations for information security

Článek I.

Article 1.

Základní povinnosti a oprávnění

Basic obligations and authorization

1. The student is authorised to use computer technology, network, and programmes within the range of his user authority and access rights. He is obliged to respect the instructions of the teacher or other personnel.
2. Žákům je zakázáno: Students are forbidden to:
 - a) Záměrně svou činností poškozovat výpočetní techniku, programové vybavení nebo jiná data. Direct their activity towards the damage of computer technology, programming, or other data.
 - b) Používat výpočetní techniku, programové vybavení nebo jiná data protiprávním způsobem nebo k protiprávní činnosti. To use computer technology, programming or other data in an illegal manner or for illegal activities.
 - c) Používat výpočetní techniku, programové vybavení nebo jiná data k činnostem namířeným proti škole či proti jakémukoliv jinému subjektu, jehož počítačové prostředky jsou dostupné prostřednictvím lokální sítě nebo prostřednictvím sítě internet. To use the computer technology, programming or other data in activities against the school, or against any other subject, whose computer environment are accesible by means of the local network or through the internet.
 - d) Umožnit přístup k výpočetní technice, programovému vybavení nebo datům osobám, které nejsou oprávněnými uživateli. To facilitate access to computer technology, programming or other data, to any unauthorised person or entity.
 - e) Používat elektronické informace a data, k nimž nemají oprávněný přístup. To use electronic information or data for which they do not have authorised access.
 - f) Kopírovat neautorizovaně a neoprávněně programové vybavení nebo jejich části. To copy, in whole or in part, any unauthorised or unapproved programmes.
 - g) Modifikovat (měnit) neautorizovaně a neoprávněně programové vybavení, data nebo připojení součástí sítě. To modify (alter) unauthorised or unapproved programmes, data, or network connections.
 - h) Odposlouchávat neoprávněně provoz (komunikaci) v síti a vytvářet kopie elektronických informací či dat procházejících jednotlivými uzly sítě, případně přenášené bezdrátovými spoji. Listen to unauthorised traffic (communications) on the network or create copies of electronic information or data forthcoming from individual tied networks, for example wireless connections
 - i) Sdělovat vlastní přihlašovací údaje jiným osobám. To share personal login data of other persons.

Článek II.

Article II

Používání výpočetní techniky

Use of the computer technology

1. Žák je oprávněn užívat pouze výpočetní techniku, která mu byla řádně předána, nebo se jedná o sdílené zařízení (např. výpočetní technika v učebně, sdílená tiskárna). The student is permitted to use only that computer technology which has been specifically allocated, or is part of the shared equipment (i.e. computer technology in a classroom, or a shared printer).
2. Výpočetní techniku je žák oprávněn užívat pouze k činnostem souvisejícím s jeho vzděláváním. The student is permitted to use the computer technology only for activities in connection with their education.
3. Pokud jde o technickou manipulaci s výpočetní technikou, nejsou žáci oprávněni ani k běžným uživatelským činnostem, jako např. výměna toneru, cartridge, doplnění papíru v tiskárně, připojení k elektrické síti a odpojení od elektrické sítě. Žákům je zakázáno rozpojovat nebo přerušovat počítačovou síť, připojovat poprvé k síti nové PC nebo jiná technická zařízení. Manipulace s výpočetní technikou, které nesmí provádět žák, zabezpečuje zaměstnanec školy. In terms of technical manipulation of computer equipment, students are not authorised even during a current user activity to, for instance, change a toner, refill a printer with paper, connect to the electrical outlets, or disconnect from the electric grid. Students are forbidden to share or interrupt the computer network, or to connect a new PC or other equipment to it
4. Závadu ve funkčnosti výpočetní techniky je uživatel povinen neprodleně oznámit učiteli nebo jinému zaměstnanci školy. Users are obliged to report defects in the function of computer technology to a teacher or other member of staff without delay.
5. Žák je povinen užívat výpočetní techniku a prostředky sítě (diskový prostor, výkon procesoru, kapacitu přenosových linek ap.) s ohledem na celkové zatížení systému. Žák je povinen neprodleně uposlechnout pokyn učitele na snížení uživatelem generované zátěže systému. The student is obliged to use computer technology and associated network (risk space, processing power, connection capacity etc.) with an overview of the full system load. The student is obliged to obey the instructions of the teacher without delay to reduce user-generated system load
6. Žák nesmí provádět změny konfigurace PC, jiných zařízení nebo zásahy do systému, které by mohly vést k jeho zhroucení, poruše nebo nežádoucímu chování. The student must not undertake any changes to the configuration of the PC, other equipment, or interventions to the system that could bring about their collapse, interruption, or undesirable behaviour.
7. Žák nesmí provést změnu konfigurace PC tak, aby se PC v síti identifikoval pod jiným jménem, než jaké mu bylo administrátorem přiděleno. The student must not undertake any changes to the configuration of the PC that would cause the PC to be identified under any name other than that designated by the administrator.
8. Práci s PC, které je připojeno do sítě, zahajuje žák přihlášením, čímž jsou mu zpřístupněny prostředky a služby dané jeho uživatelským oprávněním a přístupovými právy. Work with PC's which are connected to the network, initiates the student's agreement, thereby granting the means, services, access rights, and user authority available to him.

Článek III.

Article III

Používání programového vybavení

Using programming equipment

1. Programy je žák oprávněn užívat pouze k činnostem souvisejícím s jeho vzděláváním a pouze v souladu s licenčními podmínkami. The student is permitted to use programmes only insofar as these activities pertain to his education, and only within the constraints of licencing conditions.
2. Žákům je zakázáno instalovat jakékoliv programy: zákaz se nevztahuje na instalace na základě automatické aktualizace nabízené operačním systémem a oprávněné užívanými programy. The student is forbidden to install any programme: This restriction does not include automatic updates offered by the operating system and authorised by the programmes used.
3. Závadu ve funkčnosti programu, kterou není schopen a oprávněně řešit sám žák, je povinen neprodleně oznámit učiteli. Defects in the function of programmes that the student is not able or permitted to solve himself must be reported to the teacher without delay.

Článek IV.

Article IV.

Informační a datová bezpečnost

Information and data security

1. Žákům je zakázáno bez vědomí administrátora zasahovat do konfigurace antivirového programu. Je zakázáno aktivně vytvářet nebo šířit škodlivé programy a znemožňovat funkci ochranných programů. Students are forbidden to configure antivirus programmes without the supervision of the administrator.
2. Obdrží-li žák (na přenosném médiu, elektronickou poštou či jiným způsobem) jakoukoliv e-mailovou zprávu s příloženým souborem nebo jakýkoliv soubor, uživatel je povinen před otevřením nebo spuštěním ověřit, zda se nejedná o spustitelný soubor, či jiný spustitelný skript. V případě, že ano, je zakázáno soubor spouštět či ukládat na disk. If the student receives (by portable media, electronic post, or other means) any form of email with an attachment or other file, the user is obliged to verify if it is an executable file or script. If it is, then it is forbidden to open or run the file or to save the file to disk
3. Má-li žák podezření na napadení PC virem, neprodleně informuje učitele a dále se řídí jeho pokyny. If the student suspects that the PC is infected with a virus, he must inform the teacher without delay and follow his instructions.
4. Žák je oprávněn využívat pouze ta přístupová práva, která mu byla řádně přidělena. Pokud žák jakýmkoliv způsobem získá přístupová práva, která mu nebyla řádně přidělena (např. chybou programů nebo technického vybavení), je povinen tuto skutečnost neprodleně oznámit učiteli a takto neoprávněně získaná přístupová práva nesmí využít. Žák dále nesmí zneužít chyby jiného uživatele (např. opomenuté odhlášení) k tomu, aby v síti pracoval pod cizí identitou nebo aby využil přístupová práva náležející jinému uživateli. The student is authorised to use only those access rights which have been properly sanctioned. If the student gains unsanctioned access rights by any means (for instance programme error or

equipment malfunction), he is obliged to report this occurrence to the teacher without delay, and must not use those unapproved access rights. Further, the student must not abuse errors by other users (for instance if the users forgets to log out) in order to use the network under a different identity or to use the access rights granted to another user.

5. Je zakázáno: It is forbidden

- Informace, které by mohly vést k narušení bezpečnosti a ochrany výpočetní techniky, sítě, programů nebo dat, zpřístupnit nebo umožnit jejich zpřístupnění neoprávněným osobám anebo tyto informace zveřejnit. To grant access or enable access to unauthorised persons to information which could bring about any breach of security and protection of computer technology, network, programmes or data, or to make such information public.
- Provádět jakékoliv činnosti, které vedou nebo mohou vést ke ztrátě nebo poškození dat, která patří škole nebo jiné osobě. To undertake any action that causes, or could cause any loss or or corruption to data belonging to the school or other persons.
- Získávat data patřící jiné osobě, bez jejího vysloveného souhlasu. To obtain data belonging to another person without their expressed agreement
- Neoprávněně kopírovat nebo zálohovat data, která obsahují osobní údaje, a tato data neoprávněně vynášet mimo objekty školy nebo je oprávněně předávat jiným subjektům. To make an unauthorised copy or to store data belonging to another person, and/or to remove this data from the school premises, or to pass on such data to another person without authorisation.
- Odstranit informace, označení či zařízení identifikující nositele či vykonavatele autorských práv na daný program, autora či jinou oprávněnou osobu, nebo vytvářet či pozměňovat data s cílem ovlivnit kontrolu oprávněnosti použití daných programů. To remove or delete information, labels, or devices identifying the copyright holder or executor of the programme, the author, or other authorised person, or to create or rename data with the aim of influencing control of authorisation of the use of such a programme.

6. Při opuštění pracoviště je žák povinen zabezpečit před zneužitím PC a data, která jsou jeho prostřednictvím přístupná. Za dostačující způsob zabezpečení se považuje uzamknutí uživatelského účtu, odhlášení nebo vypnutí PC. Upon leaving the workplace, the student is obliged to secure the PC, and data to which he has access, against misuse.

7. Škola si vyhrazuje právo zaznamenávat a po dobu šesti měsíců uchovávat informace (metadata) o spojeních uskutečněných pomocí sítě školy, a to primárně z důvodu dohledávání a dokazování případných incidentů. The school reserves the right to record, and for a period of six months to store, information (metadata) about connections realised with the aid of the school network, primarily for the purpose of investigation and proof in case of incidents.

Článek VI.

Article VI.

Užívání přístupu k síti internet

The use of internet access

1. Každému žákovi je zpřístupněna, po autentizaci, prostřednictvím uživatelského PC internetová síť. Every student has access, after authentication, by means of user PC'S to the internet.

2. Ředitel školy si vyhrazuje právo zakázat nebo zablokovat přístup k některým webovým stránkám s obsahem, který není nezbytný pro vzdělávání nebo je nevhodný. The headmaster of the school reserves the right to forbid or block access to any web pages with content that is unsuitable, or is not required for educational purposes.
3. Administrátor má právo regulovat dostupnost sítě internet jednotlivým uživatelům, upravovat jejich denní kapacitní limity přijatých a odeslaných dat z a do sítě internet. The administrator has the right to regulate access to the internet network by individual users, to adjust their daily capacity limits of received and sent data to and from the internet network.

Článek VII.

Article VII.

Používání vlastní výpočetní techniky

Use of personal computer technology

1. Do školní sítě je zakázáno bez souhlasu administrátora přímo nebo nepřímo připojovat jakákoliv technická zařízení, která nejsou ve vlastnictví školy nebo k nimž škola nemá oprávnění k užívání. Without prior permission of the administrator, it is forbidden to connect directly or indirectly and kind of technical equipment which is not the property of the school, or which the school is not authorised to use.
2. Pro připojení vlastního výpočetního zařízení k síti internet může žák využít vyhrazené sítě, která je přístupná po autentizaci a je šířena zejména pomocí technologie Wi-Fi. For the connection of personal computer equipment to the internet network, the student may use the reserved network, which is accessible after authentication, and which is distributed by means of Wi-Fi technology.
3. Správce sítě zajistí bezpečné oddělení vyhrazené sítě od sítě školní, tak aby bylo znemožněno přístupu vlastních zařízení k prostředkům ve školní síti. The site administrators ensure safe separation of the reserved network from the school network, so that it is not possible to access the school network by means of personal equipment.

V Kroměříži 11. 11. 2019

Vypracoval: Mgr. Milan Budín