# PESTSZENTIMREI ADY ENDRE ÁLTALÁNOS ISKOLA

# Digitális gyermekvédelmi szabályzat 2017

**Digitális gyermekvédelmi stratégia**

A Pestszentimrei Ady Endre Általános Iskola a következő stratégiát dolgozza ki:

A program 3 alappillére:

1. Tudatosítás, megelőzés
2. Védelem, biztonság
3. Segítségnyújtás, szankció alkalmazása

## 1. Tudatosítás, megelőzés

Információ nyújtása:

- a gyerekeknek,
- a szülőknek,
- a pedagógusoknak.

A gyerekekkel meg kell beszélni, hogy milyen szabályok hivatottak őket és adataikat védeni és miért. Az eBiztonság témáját a tananyag részévé kell tenni. A következő kereteken belül és formában dolgozzuk fel a kérdéskört: osztályfőnöki óra, etika, informatika óra, külsős programok, vendégelőadók az iskolában, CSIBÉSZ Gyermekjóléti Szolgálat, iskolarendőr.
A szülőknek évente legalább egyszer szülői fórumot szervezünk, melyen a hatékony védekezés lehetőségein kívül felhívjuk a figyelmet a szülő felelősségére kiskorú gyermekének Internet és telefon használatával kapcsolatban. Ezen kívül írásbeli tájékoztatót bocsájtunk a rendelkezésre. A szűrők listáját a Honlapon is megjelentetjük.
A pedagógusok felkészültsége a felületek használatával legyen naprakész, melyet továbbképzések formájában valósítunk meg. Évente egyszer a rendőrkapitány előadásán veszünk részt.

Megtartjuk a Biztonságos Internet Napját. (február 7.)

## 2. Védelem, biztonság

- Iskolánk részt vesz az eBiztonsági minősítő programban.

Az eBiztonság Minősítés célja, hogy az internet- és eszközhasználat, az online megjelenés biztonságos legyen, az intézmény könnyen lépést tarthasson az eBiztonsági alapelvekkel, értékelhesse saját intézménye infrastruktúráját, irányelveit és gyakorlatát. Segítségével kiderül az intézmény eBiztonsági szintje, illetve hiányosságok esetén az, hogy milyen feladatok elvégzése szükséges a biztonság teljes körű kiterjesztése érdekében.

Intézményünk Bronz minősítést ért el.

A kapott akcióterv végrehajtásának határideje: 2019. április

Felelős: iskola vezetősége, rendszergazda

Az akcióterv, valamint a minősítést igazoló dokumentum ezen szabályzat 1. számú mellékletét képezi.

- Telefonok, tabletek, notebookok és egyéb infokommunikációs eszközök összegyűjtése

  Az alsós tanulók az osztályban kialakított saját szabályrendszer szerint hozhatnak be az iskolába, és használhatnak digitális eszközöket.

  A felsős tanulók fél nyolc után, iskolába érkezéskor beteszik az osztályuk kosárkájába a készüléket, melyet vagy egy tanuló, vagy legkésőbb az 1. órát tartó tanár visz a terembe. 1. óra után a tanár leviszi a tanáriba. Akkor lehet a készülékeket a tanári szobából elkérni, amikor a tanuló megy haza.

  Szükség esetén engedéllyel el lehet kérni a készüléket nap közben, felügyelet mellett lehet hazatelefonálni.
- Az iskolai számítógépek használatát a házirend mellékletét képező szabályzat határozza meg.

  A szabályzat a 2. számú mellékletben olvasható.
- A szűrőprogramok széles körű használata, az újítások nyomon követése, lehetőség szerinti telepítése fontos feladat.

  Néhány link segítségképpen: a 3. számú mellékletben található.

## 3. Segítségnyújtás, szankciók alkalmazása

**a, segítségnyújtás:**

- Az események, történések iskolába való behatása esetén értesítjük a szülőt, és segítő beszélgetésre invitáljuk az iskola gyermekvédelmi felelősével. Amennyiben iskolán kívül történő internetes zaklatásról szerzünk tudomást, az iskola segítő szándékkal

akkor is beavatkozhat. A diákokkal, szülőkkel való beszélgetés az első lépés, melyet szükség szerint követhetnek ismét felvilágosító, tájékoztató foglalkozások, vagy amennyiben ezek nem vezetnek eredményre, akkor a megfelelő jogi lépéseket megtesszük.

**b, szankciók:**

- Az iskolában rögzített és ismertetett szabályok megszegéséért alkalmazott szankciókat a házirend szabályozza. Az iskolában a telefon engedély nélküli használata esetén elvesszük a telefont, és csak nagykorú hozzátartozónak adjuk vissza. Zaklatás esetén a szükséges jogorvoslattal élünk.

**A Digitális Gyermekvédelmi Szabályzatot a tantestület elfogadta 2017. szeptember 10-én. Életbe lép 2018. szeptember 1-jén.**

Budapest, 2018. szeptember 11.

…….

Bogárné Kováts Judit
intézményvezető

1. számú melléklet


# eSafety Label - Akcióterv az alábbihoz: Pestszentimrei Ady Endre Általános Iskola

Az Értékelő lapot kitöltötte: Kormos Péter - 2017-10-27 12:59:02

Az eBiztonság minősítő portál Értékelő lapjának kitöltésével Ön egy fontos lépést tett meg intézménye eBiztonságának vizsgálata terén. Gratulálunk! Kérjük, alaposan olvassa át az Akciótervet, hogy megtudja, mit tehet az intézményi eBiztonság javítása érdekében. Az akcióterv hasznos tanácsokat és javaslatokat tartalmaz három területen: az infrastruktúra, a szabályozás és a gyakorlat terén.

## Infrastruktúra

### Technikai biztonság

- Nagyszeru, hogy az iskola minden gépe rendelkezik vírusvédelemmel. Gyozodjenek meg arról, hogy az iskolai szabályzatok rendelkeznek a vírusvédelemrol, továbbá hogy a tanárok és a tanulók pontosan betartják az iskola vonatkozó szabályait. Ha további információra van szükség, a vonatkozó adatlap a *Készülékek védelme a rosszindulatú szoftverek ellen* itt megtekintheto www.esafetylabel.eu/group/teacher/protecting-devices-against-malware.
- Az Önök iskolájában különböző szintű szűrőket használnak, és ez a gyakorlat kiváló. Ahhoz, hogy a szabályozás módja igazán jó legyen, rendszeresen frissíteni kell; vajon ez megtörténik? Milyen gyakran tiltanak le vagy tesznek elérhetővé egy-egy blokkolt oldalt? Időről időre értékelni kell, eléri-e a célját a szabályozás, és ebbe a folyamatba minden érintettet be kell vonni.
  Ezen túl tartsák észben, hogy a megfelelő tájékoztatás és a diákok különböző korosztályainak a rugalmasságra való nevelése kulcsfontosságú a biztonságos és felelősségteljes internethasználathoz. Ezért hívják össze a tanárokat egy megbeszélésre, ahol egyeztetik, hogyan ismertetik meg a diákokkal a jó és biztonságos internehasználat módját. A következő oldalon www.paneuyouth.eu találhatnak példákat olyan beszélgetésekre, amelyeket ebben a témában folytattak, tantermi szerepjátékok és csoportjátékok formájában.

### Tanulói és személyzeti hozzáférés

- Az Önök dolgozói és tanulói számára engedélyezést követően megengedett a külső adathordozók használata. Ez azonban azt feltételezi, hogy az érintett munkatársak megfelelő képzésben részesülnek, ami alapján tudják, hogy mi tekinthető biztonságos használatnak. Vajon ez a helyzet? Ahhoz, hogy a rendszert a dolgozók és a tanulók biztonságosan használhassák, A vonatkozó szabályoknak az iskolai szabályzatokban szerepelniük kell. A kapcsolódó adatlap, a *Külső adathordozók használata* megtekinthető itt www.esafetylabel.eu/group/teacher/removable-devices, ennek segítségével megbizonyosodhatnak arról, hogy a szabályozás minden szempontra kiterjed.
- Mivel a tanulók és a tanárok használhatják saját eszközeiket az iskolai hálózaton, fontos, hogy az iskola összes tagja rendszeresen áttekintse a szabályokat, amiket szükség szerint meg kell újítani. Meg kell beszélni a tanulókkal, hogy milyen szabályok hivatottak őket és adataikat védeni és miért. A szabályok inkább tükrözzék a felhasználói viselkedést mint a technológiát. A vendégeknek is legyen kötelező elolvasni a vonatkozó szabályokat, mielőtt csatlakoznak az iskolai hálózatra.

### Adatvédelem

- Iskolájában megfelelő módon különül el az oktatási és az adminisztrációs környezet. A szabályok megújításakor javasolt ellenőrizni, hogy a tanárok felkészültsége a felületek használatával kapcsolatban naprakész. Töltsék fel

vonatkozó szabályzataikat az iskola profiljára, és osszák meg a többi, eBiztonság Minősítéssel rendelkező iskolával!
- Egy-egy jelszó segítségével hozzá lehet férni az iskola számítógépes rendszeréhez, ezért a jelszavak biztonságára vonatkozó alapelveket pontosan be kell tartani. További információ és a vonatkozó adatlap *Biztonságos jelszavak* itt megtekintheto www.esafetylabel.eu/group/teacher/safe-passwords
Vegyék be ezt a gyakorlatot a szabályzatokba, és ügyeljenek arra, hogy a felhasználók az elso belépés alkalmával ne ugyanazt a jelszót kapják.

### Szoftver-licencelés

- Bizonyosodjanak meg arról, hogy az iskolában használt szoftverek legálisak, és hogy a használattal kapcsolatos engedélyeket központilag nyilvántartják. Az IT rendszer karbantartójával is egyeztetni kell, hogy a használt szoftverek ne okozzanak biztonsági problémát a rendszerben. Az iskola szabályozza a szoftverek beszerzésének módját; ajánlott a folyamatot központosítani mindenhol, ahol erre van lehetőség.
- Tekintsék át a szoftverigényekkel kapcsolatos költségvetést. Alternatív megoldásokban is gondolkozhatnak, pl. Felhő alapú szolgáltatások vagy nyílt szoftverek.

### IT menedzsment

- Jó gyakorlatnak számít, ha az infokommunikációs technológiai rendszerért felelős személy megfelelően informált az iskola számítógépein található szofverekkel kapcsolatban - ezt világosan be kell foglalni az iskolai szabályzatokba. A hálózatért felelős személynek tudnia kell garantálni azt, hogy minden a lincenc szerződéseknek megfelelően folyik, és hogy a szoftverek nem gátolják a rendszer működését.
- Nagyszerű, hogy a tanárok szoftverrel kapcsolatos kérdéseikkel felkereshetik az iskolai információs ügyfélszolgálatot. Vizsgálják meg, hogy szükséges-e olyan képzéseket szervezni és/vagy útmutatást nyújtani, amelyekkel az iskolai számítógépekre újonnan felszerelt szoftverek használatát segítik. Fontos biztosítani, hogy az iskola tagjai ki tudják használni az új lehetőségeket, de ugyanakkor legyenek tudatában az ezekkel kapcsolatos biztonsági és adatvédelmi kérdéseknek.

## Szabályok

### Felhasználói Szabályzat (FSZ)

- Nagyszerű, hogy az iskolában érvényben van egy, az informatikai rendszer használatát szabályozó szabályzat, ami a tanulókra vonatkozik. Egészítsék ki a szabályzatot, és foglalják bele a kollégákat és más lehetséges felhasználókat is. Annak érdekében, hogy a felülvizsgált szabályzat mindenre kiterjedjen, tanulmányozzák az adatlapot és az ellenőrzőlistát *Felhasználói Szabályzat* itt www.esafetylabel.eu/group/teacher/acceptable-use-policy.
- Megfelelő gyakorlatot alkalmaznak akkor, amikor az iskola irányelveit érintő változások bevezetésekor az irányelveket azonnal frissítik. Figyeljenek azonban arra is, hogy iskolán kívüli változások, például új törvények vagy változó technológiák is befolyásolhatják az irányelveket. Ezért kérjük, legalább évente vizsgálják felül az iskola irányelveit.

### Jelentés és incidenskezelés

- Egyértelműen kell szabályozni azt a gyakorlatot, amely a potenciálisan illegális tartalmak kezelésére vonatkozik; figyelembe kell venni a kérdés jogi vonatkozásait is. Az iskola tapasztaltabb tanárai közül ki kell jelölni egy felelőst az ilyen kérdések kezelésére, és a folyamatról egyértelmű tájékoztatást kell adni a dolgozóknak és a tanulóknak az iskolai szabályzatokban/házirendben. Ne feledkezzenek meg arról, hogy a gyanús, potenciálisan illegális tartalmakat jelentsék a nemzeti INHOPE vonalon, a Nemzeti Média-és Hírközlési Hatóság által üzemeltetett felületen: (Internet Hotline).
- Online bántalmazással kapcsolatos minden incidenst központilag tartsanak nyilván, ezzel tudják tájékoztatni az iskola dolgozóit az esetleg felmerülő ügyek következményeiről és az érintett tanulók köréről, életkoráról stb. Ne mulasszák el továbbá kitölteni az eBiztonság Minősítés űrlapját: Incidensek kezelése. Ezáltal hozzájárulnak egy olyan európai adatbázis létrejöttéhez, amely az incidensek sikeres kezelésének gyakorlatait gyűjti egybe, ezzel segítve a jövőbeli munkát.

### Személyzeti szabályzat

- Lennie kell egy olyan szabályzatnak, amely a dolgozók számára világosan részletezi az elfogadható online viselkedés jellemzőt. Ezeket az információkat meg kell osztani a kollégákkal és a tanulókkal a szabályzatokban/házirendben. A dokumentumokat rendszeresen vizsgálják felül, és szükség szerint frissítsék.
- Az olyan új technológiák, mint az oktostelefonok vagy egyéb mobileszközök újfajta veszélyeket is implikálnak. Ügyeljenek arra, hogy ezeknek a tanárok tudatában vannak. Ezáltal az eszközök használata közben elkerülhetik a veszélyeket, és a diákokat is felvilágosíthatják.

### Diákok gyakorlata/viselkedése

- Önök meghatározták az elektronikus kommunikáció szabályait az iskolai szabályzatokban, ez pedig jó gyakorlat lehet más iskolák számára. Esetleg készítsenek egy segédanyagot az elektronikus kommunikáció tanulókra vonatkozó szabályairól, és töltsék fel az iskola profiljára azIskolám felülete oldalon, hogy más iskolák is hasznát vehessék az Önök tapasztalatának.
- A tanterv túl szoros ahhoz, hogy a diákok az iskolai feladatokat aszerint formálják, hogy éppen mi zajlik a napi életükben. Ez fontos, ugyanis a diákok aktívabb részesei lesznek a tevékenységnek, a tanárnak pedig lehetősége nyílik arra, hogy figyelembe vegye a valós élet dolgait. Járjanak utána a fordított tanterem lehetőségeinek és/vagy engedjék meg a diákoknak, hogy a médiafelhasználási szokásaikról és problémáikról házi feladatként információkat oszthassanak meg.

### Online iskolai jelenlét

- Vizsgálják felül a tanulókról, tanárokról és szülőkről, illetve az általuk készített fényképekre és digitális képekre vonatkozó szabályokat, és vizsgálják meg, összhangban van-e a szabályzás a legutóbbi változásokkal. Ideális esetben a szabályzat inkább foglalkozik a felhasználói szokásokkal, mint a technológiákkal. A vonatkozó adatlap *Fényképek és videofelvételek készítése és nyilvánosságra hozatala az iskolában* ( www.esafetylabel.eu/group/teacher/photos-videos) jó kiindulási alappal szolgál.
- Bár az iskolának van online jelenléte, a diákoknak nincs lehetősége ennek formálására. Járjanak utána azoknak a lehetőségeknek, amelyekkel a diákokat is be lehetne vonni, például egy digitális tanácson keresztül. Ez nagyszerű lehetőséget nyújt arra, hogy a média-írástudásról és az ezzel kapcsolatos kérdésekről tájékozódjanak. Segíthet az is, ha megszerveznek egy kortárs segítő csoportot. Tudjanak meg többet Az iskola a közösségi oldalakon kérdésről az eBiztonság adatlapján.

## Gyakorlat

### eBiztonság menedzsment

- Amellett, hogy van egy hálózati biztonsági és felhasználói adatvédelmi ellenorzésekért felelos személy, szükséges az is, hogy az iskolák rendszeres idoközönként felülvizsgálatot tartsanak, és ellenorizzék a folyamatot. Ezek nélkül ugyanis az iskola támadásoknak lehet kitéve. A vonatkozó adatlap *Iskolai szabályzat* itt megtalálható www.esafetylabel.eu/group/teacher/school-policy
  Noha helyes, hogy van egy olyan személy, aki az eBiztonsággal kapcsolatos kérdésekért felelos, az iskola minden tagjának közös felelossége, hogy a bizalmas információkat napi munkájuk során megfelelo módon kezeljék. Még azoknak a munkatársaknak is szükséges megismerkedni a kockázatokkal és a veszélyekkel, akik nem vesznek közvetlenül részt az adatkezelésben. Tanulmányozzák az adatlapot: *Felhasználói szabályzat* ( www.esafetylabel.eu/group/teacher/acceptable-use-policy), hogy mindenki megtegyen minden tole elvárhatót a digitális biztonság érdekében.
- Fontolják meg annak a lehetőségét, hogy az iskolai vezetőség/tanács egy tagját kinevezik az eBiztonsági ügyekben felelős kapcsolattartónak. Fontolják meg azt is, hogy amikor évente felülvizsgálják az iskolai szabályzatokat, olyankor egyúttal a vezetőségnek éves jelentést írnak arról, hogy hány és milyen jellegű eBiztonsági incidens történt az adott időszakban. A vonatkozó adatlap: *Iskolai Szabályzat* www.esafetylabel.eu/group/teacher/school-policy.

### eBiztonság a tantervben

- Az eBiztonság témáját a tananyag részévé kell tenni, attól függetlenül, hogy ez az Önök országában előírás-e vagy

sem. Sok olyan jó gyakorlat létezik, amely szabadon hozzáférhető, és segíti ennek megvalósítását. További információkat a vonatkozó adatlapon találnak *eBiztonság a tananyagba* itt www.esafetylabel.eu/group/teacher/esafety-in-curriculum.

- Győződjenek meg arról, a hogy az eBiztonsági tananyag lépést tart az újdonságokkal - ehhez használjanak minden hozzáférhető forrást, és ügyeljenek arra, hogy a tananyag tapasztalatokra épüljön, hiszen a tanulókat a technológia használati szokásaiktól függően más és más információval kell ellátni.

**Iskolán kívüli tevékenységek**

- Nagyszerű, hogy a tanulóknak a tanórákon kívül is nyújtanak eBiztonsági segítséget, ha ezt kérik. Fontolják meg annak lehetőségét, hogy minden tanulónak eBiztonsággal kapcsolatos segítséget nyújtsanak. Érdemes nekik segíteni abban, hogy beállításaikkal védeni tudják Facebook oldalukat stb. Az eBiztonság Minősítés portálon hasznos információkat találhatnak a témában; tanulmányozzák az adatlapot *A tanulók technológiahasználata az iskolán kívül* itt www.esafetylabel.eu/group/teacher/social-media-pupils.
- Használják fel a Biztonságos Internet Napját arra, hogy az egész iskolát mozgósítsák az online biztonság ügyéért. Információt és háttéranyagot itt találnak: www.saferinternetday.org; ideális lehetőségük nyílik arra, hogy a tanulókat egymás segítésére buzdítsák.

**Háttéranyagok**

- A dolgozók közül mindenki legyen felelős valamilyen eBiztonsággal kapcsolatos ügyért. Az iskolában dolgozó tanácsadók, egészségügyi dolgozók stb. helyzetükből kifolyólag tudnak tanácsot és javaslatokat adni ezekben a témákban, ezért be kell őket vonni az iskolai szabályzatok rendszeres fejlesztésébe és felülvizsgálatába. Érdemes megfontolni azt is, hogy ezek a dolgozók képzésben is részesülhessenek.
- Nagyszerű, hogy van olyan munkatársuk, aki járatos az eBiztonsággal kapcsolatos témákban, és akihez bizalommal fordulhatnak a diákok.

**Személyzeti képzés**

- Az Önök iskolájában a dolgozók nem részesülnek eBiztonsági képzésben, pedig rendszeresen tájékoztatni érdemes őket az újabb trendekről. Próbálják meg felmérni az igényeket, hogy meg tudják határozni, mit várnak el a különböző dolgozók a képzéstől. Tájékozódjanak az eBiztonság Minősítés portálon a javasolt képzésekkel kapcsolatban itt www.esafetylabel.eu/group/teacher/esafety-training-courses.
- Fontos, hogy a tanárok ismerjék azokat a technológiákat, amelyekkel diákjaik a szabadidejüket töltik. Ez fontos, ugyanis ez a tudatosság jelenti az első lépést abba az irányba, hogy az iskola foglalkozzon a diákok iskolán kívüli eszközhasználatával. Ugyanakkor ne kérjék a diákokat arra, hogy házi feladatukat olyan technológiákkal készítsék el, amelyek az iskolán kívül számukra elérhetetlenek. Ügyeljenek arra, hogy minden tanár értesüljön ezekről a kérdésekről. Nézzék meg a következő felmérést: Essie iskolai IKT felmérés.

Az Ön által kitöltött Értékelő lapot egy számos kérdést tartalmazó adatbázisból generáltuk. Számunkra az is fontos, hogy megtudjuk, fejlődnek-e az eBiztonság azon területei, amelyeket a kérdőív nem érintett. A fejlődés tényét alátámasztó dokumentumokat feltöltheti itt: Bizonyíték feltöltése az eBiztonság Minősítés portálIskolám felülete részén. Ne feledje, hogy az Értékelő lap kitöltése csak a minősítési folyamat első része, mivel az alátámasztó dokumentumok feltöltését, a tapasztalatcserét a Fórumon, és a sablon segítségével történő incidensek jelentését mind figyelembe vesszük a minősítés során.


Az iskola megkapta az
eBiztonság
Minősítést
bronz
Érvényes: 2019.04.


Az iskola megkapta az
eBiztonság
Minősítést
bronz
Érvényes: 2019.04.


Az iskola megkapta az
eBiztonság
Minősítést
bronz
Érvényes: 2019.04.

2.számú melléklet

# Az iskolai számítógépes hálózat használatának rendje

- A számítógépek elsődleges célja az iskolában folyó oktatási, tanulási folyamat segítése, technikai feltételeinek biztosítása. Ezért minden olyan tevékenység elsőbbséget élvez, amely ennek a célnak felel meg.
- Az alábbi szabályok az iskola minden tanulójára és dolgozójára kötelező érvényűek.
- A felhasználók a számítógépek használatával elfogadják és magukra nézve kötelezőnek tekintik a hálózat használatának rendjét.
- A számítógépes hálózat használati rendjének megsértése fegyelmi vétség, amely súlyának megfelelő fegyelmi intézkedést von maga után.

**Hozzáférés a hálózathoz**

- A hálózat felhasználóinak nyilvántartása, a belépések engedélyezése és tiltása a rendszergazda feladata, egyben a hálózat biztonságos működésének alapfeltétele. A felhasználói azonosítók létrehozása és törlése a rendszergazda joga.
- Azonosítót kérhet az iskola minden tanára, nem pedagógus dolgozója, akit a hálózat használatától korábban nem tiltottak el. Indokolt esetben a rendszergazda más személynek is adhat azonosítót.
- A tanulók saját eszközeikkel (telefon/tablet) nem használhatják!
- A jelszavakat (e-mail. nyomtató kód, laptop) másokkal közölni, használatát másnak akár rövid időre is lehetővé tenni tilos! Ezekből adódó károkért felelősséget nem vállalunk! (pl: új nyomtatókód feltöltés) Ha felmerül a gyanúja, hogy a jelszót valaki megtudta, akkor azonnal meg kell változtatni, és haladéktalanul tájékoztatni kell a rendszergazdát.
- A tanulói vagy dolgozói munkaviszony megszűnésével egyidejűleg a rendszergazda törli a felhasználó könyvtárát, és minden hozzáférését.

**A számítógépes hálózat használatának szabályai**

- Valamennyi felhasználó felelős az egész hálózat biztonságáért, tevékenységével nem akadályozhatja, nem veszélyeztetheti a hálózat működését.
- A felhasználók a hálózat hardver és szoftver eszközeiért anyagi felelősséggel tartoznak.
- A szándékosan, vagy a felhasználó hibájából okozott kárt a károkozó köteles megtéríteni, mások károkozását megakadályozni, illetve jelenteni a rendszergazdának vagy az iskola igazgatójának.
- A felhasználók a többi felhasználó tevékenységét, személyiségi jogait (pl. sértő, öncélú üzenetek küldése, e-mail, sms) és az óra menetét (az előírt programtól eltérő programok engedély nélküli használata) nem zavarhatják.
- A felhasználó csak szabályos kijelentkezés után állhat fel a gép mellől. Ennek elmulasztása a belépési jog felfüggesztését eredményezheti. A gépet lehetőleg csak az utolsó óra végén kapcsolják ki.

**A felhasználók jogai**

A felhasználók

- Ésszerű mértékben (néhány (megabyte/MB) használhatják hálózati mappájukat állományaik tárolására. Ha a merevlemez kapacitáshiánya nem igényli, nem vezetünk be korlátozást a felhasználható terület méretére vonatkozóan, de fenntartjuk a jogot a nagyméretű mappák és állományok figyelmeztetés utáni törlésére.
- Használhatják a szervereken elhelyezett nyilvános programokat és más állományokat.

- Külön engedély nélkül is használhatják a hálózat rendelkezésre álló szolgáltatásait, ha ezzel a jelen szabályzat előírásait, a jogszabályokat, az általános erkölcsi normákat és a Netikettet, illetve más felhasználók érdekeit nem sértik.
- Használhatják a World Wide Webet és más internetes szolgáltatásokat, kivéve a pornográf, szélsőséges nézeteket valló, rasszista vagy bármilyen módon erőszakra buzdító vagy jogellenes anyagok letöltését.
- Saját honlapot készíthetnek, melyet a rendszergazda helyez el az iskola web szerverére. A weblapok tartalma nem sértheti az iskolánk jó hírét és a jogszabályokat.

**A felhasználók kötelességei**

- A felhasználók kötelessége, hogy a hálózat biztonságának hiányosságaira felhívja a rendszergazda figyelmét.
- Köteles a saját állományairól biztonsági másolatot készíteni és az iskolai hálózattól függetlenül tárolni. A szervereken tárolt állományok sérüléséért, megsemmisüléséért az iskola semmilyen felelősséget nem vállal.
- A felhasználó köteles továbbá a hálózat működésében tapasztalt rendellenességeket, a tudomására jutott jelszószerzési és betörési kísérleteket haladéktalanul jelezni a rendszergazdának.
- A felhasználók kötelessége, hogy a belső és az internetes hálózati erőforrásokkal takarékosan, másokra is tekintettel bánjanak. Ilyen erőforrások például a lemezterület, a sávszélesség. Csak olyan dolgokat töltsünk le az Internetről, amelyekre elengedhetetlenül szükségünk van, illetve amire a tanárok utasítást adnak és helyben nem hozzáférhetők.

**A felhasználók számára tilos:**

- a perifériák csatlakozóit kihúzni, rongálni (egerek, billentyűzetek, gépház, monitort) pendrive kivételével a felügyelő engedélye nélkül külső eszközöket csatlakoztatni. Az eszköz helytelen csatlakozásából eredő meghibásodásáért az iskola felelősséget nem vállal, a számítógépekben keletkező károkat a felhasználónak meg kell térítenie.
- a Windows grafikus felületének módosítása (háttérkép, Start menü stb.).Kivéve ha az óra témája az ilyen módosítások gyakorlása, akkor az óra végén vissza kell állítani az eredeti beállításokat.
- a hálózat hardver- és szoftverkonfigurációjának (a gép neve, IP-címe stb.) módosítása.
- az iskola tulajdonát képező programok illegális lemásolása.
- a hálózatot az Internet veszélyeztetésére vagy mások munkájának hátráltatására használni. Vírusok, kémprogramok, szerkesztése, és terjesztése szigorúan tilos!
- a hálózaton jogellenes, rasszista vagy erőszakra buzdító, szeméremsértő, politikai vagy a szerzői jogokat sértő anyagokat tárolni, ilyeneket az Internetre kiajánlani vagy az Internetről letölteni, a levelezőrendszert ilyen anyagok forgalmazására használni.
- „feltört” programok letöltése az Internetről.
- crack, kódok, programindító kulcsok letöltése. A tilalmak nemcsak a programokra, hanem minden szerzői joggal védett termékre, például filmekre, zenei anyagokra is kiterjednek.
- A gépekre csak az informatika-tanárokkal, illetve a rendszergazdával egyeztetett szoftver telepíthető. Bizonytalan eredetű szoftver telepítése esetén kötelező a vírusmentességet ellenőrizni. Szoftverek engedély nélküli telepítése súlyos fegyelmi vétségnek minősül.

- **Szigorúan tilos** a hálózati vagy lokális háttértárakon a rendszergazda engedélye nélkül játékprogramot tartani.

**A legszigorúbban tilos** és a hálózat használatától való azonnali és végleges eltiltással jár:

- a más nevében való bejelentkezési kísérlet még akkor is, ha az illető engedélyével történik.
- más azonosítójának, jelszavának használata, illetve a jelszó kölcsönadása (a kölcsönadásban mind a két fél vétkes!). A jelszóval elkövetett visszaélésekért a felelősség a jelszó tulajdonosát terheli.
- más jelszavának kiderítésére, állományainak, leveleinek illetéktelen elolvasására vagy módosítására tett kísérlet (ha ketten ülnek egy gépnél a tanórán, akkor is legyenek tekintettel egymás jelszavának titkosságára).
- jogosulatlan belépési kísérlet külső intézmény hálózatába.
- a hálózat biztonsági rendszerének esetleges hibáival való visszaélés.

**A teremhasználat rendje**

- A számítógéptermekben diákok csak felügyelet mellet tartózkodhatnak. Felügyelő személynek minősülnek az iskola tanárai, és a rendszergazda.
- A felügyelő személy kötelessége a felhasználók ellenőrzése, feladata a terem- és hálózathasználat rendjének fenntartása. A felhasználók kötelesek betartani a felügyelő személy utasításait.
- A teremben semmiféle étel, ital nem fogyasztható, s nem tárolható a számítógépek környezetében!
- Nem vihető be a terembe (táska, szatyor, hátizsák stb.), azokat a folyosón ZÁRT állapotban kell tárolni.
- Az óra végén a tanár köteles ellenőrizni, hogy az órán részt vett tanulók rendben, hiánytalanul hagyták-e a számítógépeket, illetve a hozzá kapcsolódó eszközöket, és kijelentkeztek-e a hálózatból. Miután minden diák elhagyta a termet, az ajtót be kell zárni.
- A géptermet tanórán kívül a diákok a délutáni szakkörökön, felügyelet mellett vehetik igénybe. Szabad gép hiányában prioritást élvez az a felhasználó, akik iskolai munkáját végzi (házi feladat, kiselőadás, versenyre való felkészülés stb.).
- A rendszergazda karbantartás céljából vagy a hálózat normális működésének ellenőrzésére bármikor bármelyik gépet igénybe veheti, sürgős esetben akár az ott folyó munkát megzavarhatja.

Budapest, 2017. szeptember 1.

**A könyvtári számítógépek használatának szabályai**

- A számítógépeket csak felügyelettel, a könyvtár nyitvatartási idejében használhatod.
- Előnyt élvezel abban az esetben, ha a könyvtárossal előre időpontot egyeztetsz.
- A számítógép használatának kezdetét és befejezését jelezd a könyvtárosnak.
- A számítógép-használat nem csoportfoglalkozás, egyedül ülj mellette.
- A gépek ki- és bekapcsolását, valamint újraindítását bízd a könyvtárosra.
- Kérlek, hogy minden hibát, üzemzavart jelezz!
- A másolás csak adathordózóra lehetséges. Ennek menetét beszéld meg a könyvtárossal.
- A számítógép beállításait (rendszer, képernyőkímélő, háttér, jelszó, böngésző, kezdőlap stb.) ne változtasd meg!
- A könyvtári számítógépeken nem szabad chat-elni (csetelni), valamint a jó ízlést sértő Internetes oldalakon böngészni.
- A fenti szabályok megsértése esetén – hosszabb vagy rövidebb ideig – eltiltunk a könyvtári számítógépek használatától.

…….

könyvtáros

A számítógépek használatának szabályait elolvastam. Tudomásul vettem és magamra nézve kötelezőnek tartom.

.....

tanuló.....

3.számú melléklet

Szűrőprogramok:
http://mte.hu/gyermekbarat-internet/szuroprogramok-mobiltelefonokra/"http://mte.hu/gyermekbarat-internet/szuroprogramok-mobiltelefonokra//a
http://mte.hu/gyermekbarat-internet/internetes-szuroprogramok/"http://mte.hu/gyermekbarat-internet/internetes-szuroprogramok//a

Fontos linkek a témában:
http://buvosvolgy.hu/"http://buvosvolgy.hu//a
http://buvosvolgy.hu/cikk/118/Kiadvanyok"http://buvosvolgy.hu/cikk/118/Kiadvanyok/a
http://mte.hu/gyermekbarat-internet/"http://mte.hu/gyermekbarat-internet//a
https://www.digitaliscsalad.hu/"https://www.digitaliscsalad.hu//a

Chrome - a böngészőbe beépülő modulok (letölthetőek a chrome Internetes áruházból):
Safe Lagoon – Parental control
eSafely

Androidra:
https://play.google.com/store/apps/details?id=com.kaspersky.safekids"https://play.google.com/store/apps/details?id=com.kaspersky.safekids/a (fizetős és ingyenes verzió)
https://play.google.com/store/apps/details?id=com.mcafee.security.safefamily"https://play.google.com/store/apps/details?id=com.mcafee.security.safefamily/a

Szülői felügyelet használata iPhone, iPad és iPod touch készüléken:
https://support.apple.com/hu-hu/HT201304"https://support.apple.com/hu-hu/HT201304/a

Bármilyen típusú mobiltelefonon (android, windows, iphone) keresőkifejezésnek a Parental Control vagy kid control kifejezést javaslom beírni. Számtalan találat közül választhatunk. A programok értékelésénél itt érdemes figyelembe venni, hogy

gyerekek is értékelhetnek, ők nyilván nem örülnek ezeknek, és lefelé húzzák a pontszámokat

Firefoxot használóknak: https://addons.mozilla.org/en-US/firefox/addon/kidzui/"https://addons.mozilla.org/en-US/firefox/addon/kidzui//a

Fontos linkek a témában:
http://saferinternet.hu/"http://saferinternet.hu//a
http://buvosvolgy.hu/"http://buvosvolgy.hu//a
http://buvosvolgy.hu/cikk/118/Kiadvanyok"http://buvosvolgy.hu/cikk/118/Kiadvanyok/a
http://mte.hu/gyermekbarat-internet/"http://mte.hu/gyermekbarat-internet//a
https://www.digitaliscsalad.hu/"https://www.digitaliscsalad.hu//a

További szűrőprogramok (angol nyelven):
https://www.pcmag.com/article2/0"https://www.pcmag.com/article2/0/a,2817,2346997,00.asp