



Утвърждавам
Зорка Петкова
Директор
Заповед №18/23.09.2020 г.

Правила за работа в електронна среда

Настоящите правила се създават при прилагане на чл. 115а от Закона за предучилищното и училищното образование във връзка със световната пандемия от корона вирус COVID 19.

Правилата за работа в електронна среда са в сила и след прекратяване на извънредната епидемична обстановка.

I. Правила за работа на учителите в електронна среда при обучение на ученици

1. Препоръчва се обучението на учениците да се осъществява от учителите с електронни платформи, тъй като те предоставят възможност за по-пълноценно обучение и улесняват отчетността.

2. Интернет приложения, социални мрежи или електронна поща се използват за връзка с родителите.

3. при използване на затворена група за връзка с родители, учителите следва да изпишат на видно място: не може да се копира, разпространява, коментира съдържанието от провежданата комуникация без изричното съгласие на всеки един член на групата;

4. не следва да се използват за образователни цели приложения, които предоставят достъп до лична информация на участниците -включително снимки, адреси и т.н.

5. за индивидуална консултация може да се използва e-mail, телефон;

6. Учителят, който осъществява обучение в електронна среда на ученици от ОУ „Христо Ботев” - с. Мъглен, общ. Айтос е длъжен:

преди:

6.1. създаването на затворена група за комуникация с родители в социалните мрежи, с цел публикуване на материали за обучение на ученици и преди ползване на образователна платформа за обучение на ученици, да уведоми писмено директора за намеренията си и да изчака одобрение;

след:

6.2. създаването на затворена група за комуникация с родители в социалните мрежи, с цел публикуване на материали за обучение на ученици и при ползването на образователна платформа за обучение на ученици, да уведоми писмено директора за начина, по който той може да бъде включен към групата или образователната платформа.

6.3. Т. 6.1. и т. 6.2. се въвеждат в съответствие на чл. 258, ал. 1 от ЗПУО.

7. При започване на работа с ученици в образователна платформа или затворена група в социалните мрежи всеки учител е длъжен да запознае учениците и техните родители съответно с т. I и т. II от настоящите правила;

8. Учителят е длъжен в случай, че забележи нарушение на някои от правилата от т. II да уведоми директора, родителите на ученика и да проведе разговор с ученика и психолога на училището, за работа в безопасна електронна среда.

II. Правила за опазване на личните данни на учениците при работа в интернет.

Учениците:

1. Да не предоставят лична информация като име, парола, адрес, домашен телефон, месторабота и служебен телефон на родителите си или училището, в което учиш.
2. Да не изпращат свои снимки или снимки на свои близки, без преди това да са обсъдили решението си със своите родители.
3. Винаги преди да качат своя снимка и/или да публикуват своя мобилен номер, да помислят добре дали искат и ще е добре ли за тях тази информация да стане достъпна за един неограничен кръг от хора.
4. Да не приемат среща с някого, с когото са се запознали в интернет, без знанието на родителите си. Ако те одобряват срещата, нека тя да е на публично и оживено място и задължително да е в присъствие на техни близки или приятели.
5. Не отговарят на съобщения, които са обидни, заплашващи, неприлични или ги карат да се чувстваш неудобно. Информират родителите си или друг техен близък възрастен човек за такива съобщения и за техния източник.
6. Не отварят приложения на електронна поща, получени от непознат подател. Те могат да съдържат вирус или програма, която да увреди техния компютър или да черпи неограничено информация от него.
7. Внимават, когато някой им предлага нещо безплатно или ги кани да се включат в дейност, обещаваща лесна, бърза и голяма печалба. В тези случаи, най-вероятно, става дума за измама.
8. Са внимателни и наблюдателни при попълване на регистрационните форми при извършване на регистрация в интернет сайтове.
9. При регистрации винаги проверяват има ли данни на сайта относно администратора/модераторите, които го поддържат, както и възможност за обратна връзка с тях - адрес за контакт.
10. Четат „Условията за ползване“ на сайта, преди да се съгласят с тях! Там трябва да бъде предоставена информация относно необходимостта и целта на събирането на лични

данни на потребителя. В случай че такава информация не е предоставена и не им е предоставена възможност да се обърнат към администратора/модераторите на съответния сайт или в тях се съдържа информация, която притеснява децата, то тогава сигнализират на горещите линии, като подадат оплакване. Трябва да знаят, че всеки администратор/модератор, който поддържа конкретен сайт, е длъжен да даде информация относно това за какво са му необходими личните данни на потребителите, за какво ще ги ползва, за какъв срок, какво ще се случи с тях, когато те вече няма да са му необходими за тази цел, за която са му ги предоставил (например регистрация), както и на кого и поради какви причини той ще може да ги даде.

11. Не четат и не разглеждат сайтове, които съдържат материали с вредно или незаконно съдържание. Единственото нещо, което те биха могли да им донесат са вреди, неприятности и проблеми. Няма нищо грешно и лошо в това, че от чисто любопитство, случайно или по съвет от „приятел“ в нета са достъпили сайт с вредно или незаконно съдържание. Необходимо е без притеснение да споделят това с родител или друг техен близък възрастен човек. Именно той ще им даде най-добрия съвет как да постъпят в тази ситуация.

Какво означава „сайт с вредно съдържание“?

Това са интернет страници, чието съдържание оказва или би могло да доведе да травмиращо психично въздействие или да подтикне техните ползватели към поведение, водещо до психични и/или физически травми.

Какво означава „сайт с незаконно съдържание“?

Това са интернет страници, на които е публикуван или качен материал, за който в закон е предвидена забрана и се носи съответната отговорност.

12. Използват на максимум възможностите, които предоставя конкретният сайт за социални контакти за защита на профила си и информацията, която са качили на него.

13. Внимават, когато разговарят в чат, дискуссионни форуми, социални мрежи и т.н. Помнят, че хората онлайн често могат да се представят за такива, каквито не са. Важно е да знаят, че възможността, която предоставя мрежата на теб да останеш анонимен или да се представиш за друг, се предоставя и на всички други участници в нета!

14. Нещата, които правят в Интернет, не трябва да вредят на други хора или да противоречат на законите. Трябва да бъдат вежливи и да уважават правата и достойнството на другите участници в интернет.

15. Консултират се с родителите си, преди да свалят или инсталират нова програма на компютъра си. Не правят нищо, което може да увреди компютъра им или чрез дадено действие от тяхна страна да се разкрият данни за тях и семейството им.

16.Споделят с родителите си или с друг възрастен техен близък за начините, чрез които се забавляват, информират се и научават нови неща от Интернет.

17.Разумни и изобретателни са при избора си на пароли. Помнят: Паролите трябва да се променят периодично. Колкото по-дълго време използват една и съща парола, толкова по-голям е рискът тя да бъде разкрита.

18.Използват антивирусен софтуер. Обновяват го редовно и не забравят да сканират компютъра периодично.

19.В случай, че попаднат на информация или други неща в Мрежата, които не им харесват или ги плашат по някакъв начин и нямат възможност да го споделят с родител или с друг близък възрастен, то тогава могат да подадат сигнал на адрес: <http://web1.12.net/>, <http://www.safenet.bg/> или <http://www.cybercrime.bg/bg>.

III. СЪВЕТИ ЗА РОДИТЕЛИ

Посъветвайте вашето дете:

1. Да не дава лична информация като име, парола, адрес, домашен телефон, училището, в което учи, месторабота или служебен телефон на родителите си, както и друга лична информация за себе си, приятелите си, за вас, за братя, сестри или други роднини и близки без вашето или тяхно изрично разрешение.

2. Да не приема среща с някого, с когото се е запознал чрез социалните мрежи, сайтовете за запознанства, форумите, чат програмите или по друг начин чрез интернет, без вашето знание и съгласие. Трябва да знае, че един човек може да има няколко регистрирани профила и винаги може да се представи за някой друг. За това е необходимо отделяне на специално внимание към тази категория сайтове с оглед на сигурността на детето.

3. Да не отваря и да не отговаря на електронни съобщения/писма, получени от непознат подател, тъй като те могат да съдържат вирус или друга програма, която да увреди софтуера или хардуера на компютъра, както и да позволи безпрепятствен достъп до съдържащата се в него информация.

4. Да не отговаря на съобщения, които са обидни, заплашващи, неприлични или го карат да се чувства неудобно и във всички тези случаи да ви информира за такива съобщения.

5. Да не изпраща свои снимки или снимки на свои близки, без преди това да е обсъдил решението си с вас. Обърнете му внимание, че публикуването на негови снимки или качването на видео в социалните мрежи и сайтовете за запознанства прави достъпни тези материали за огромен кръг от хора. Включването на уеб камера в реално време при разговор с непознат в чат програмите води до същия ефект. Лесният достъп до публикувани снимки или видеоматериали може да даде възможност на хора, които искат да му навредят, да ги използват по начин, който да го злепостави.

6. Да не се доверява на хора, с които се познава от и общува във виртуалния свят, да не споделя с тях свои или на близките си лични данни, които могат да бъдат от различно естество, но в своята съвкупност да доведат до идентификация на детето или на неговите родители, братя, сестри, приятели и др. Изострете му вниманието върху, това да не предоставя и да не публикува собственото си име или това на близки и приятели, адрес, данни за училището, в което учат, телефон /стационарен или мобилен/. Предоставянето или публикуването на името и адреса на дома и/или училището, в което учи, в интернет ще даде възможност на всеки, който има за цел да го открие в реалния свят, да го идентифицира и да стигне до него. Опасността, която крие предоставянето на телефонният номер, било стационарен или мобилен, може да доведе до телефонен тормоз от страна на злонамерени хора, както и да бъде използван от тях за злепоставящи действия и публикации в нета и извън него.
7. Да се консултира с вас винаги преди да сваля или инсталира нова програма или друг софтуер на компютъра.
8. Да внимава и да се съобразява с правилото - нещата, които прави в Интернет, да не вредят на други хора или да противоречат на законите.
9. Да внимава, когато създава нови познанства и провежда разговори в чата -хората онлайн често се представят за такива, каквито не са.
10. Да споделя с вас начините, чрез които се забавлява, игрите, които харесва, и новите неща, които научава от Интернет.
11. Да пази паролите си, да не ги споделя с никого и да ги променя периодично.
12. В случай, че попадне на информация, която го плаши или го притесни по един или друг повод, да сподели това с вас или да подаде сигнал на горещата линия за безопасен интернет: <http://web112.net/>, <http://www.safenet.bg/> или <http://www.cybercrime.bg/> чрез предвидения за тази цел паник бутон.

Какво може да направите, за да се погрижите за безопасността на детето в интернет

Поемете лична отговорност за безопасността на детето си в Интернет.

Наложете правила за безопасно ползване на Интернет и следете за тяхното стриктно спазване.

Поставете компютъра в обща стая/помещение. Поставянето на компютъра в общо помещение ще ви даде възможност да станете „страничен“ и „недосаждащ“ свидетел на посещаваните интернет страници от детето, както и на всички извършени от него посещения, действия, дискусии и т.н. поне за периода от време, през който сте заедно.

Провеждайте периодични разговори с детето за опасностите, които крие интернет, и начините, по които то може да се защити. Обяснете му колко е важно да пази личните си

данни и тези на своите близки, роднини и приятели и да не ги предоставя на „онлайн приятели“, като говорите с него свободно относно злоупотребите, за които могат да бъдат използвани те.

Създайте потребителски профил на детето си на компютъра в къщи. Децата трябва да имат собствени акаунти на компютъра. Това е много ефикасен начин за контрол на дейностите им в интернет. И още нещо: администратор на домашния компютър трябва задължително да бъде възрастен човек. Акаунта на детето задължително трябва да бъде без или с ограничени администраторски права.

Инсталирайте програма за родителски контрол - програмата за родителски контрол ще ви предостави възможност да ограничите достъпа на вашето дете до сайтове с неподходящо за него съдържание, да наложите времеви рестрикции за ползване на компютъра, да блокирате ползването на определени програми и т.н.

Прекарвайте повече време със своите деца, като: играете на предпочитаните от тях компютърни игри или разглеждате интересните за тях интернет страници - така ще разберете за навиците им, и за тяхното поведение в мрежата, за желанията и интересите им.

Сърфирайте заедно в Интернет и едновременно с това ги учите на безопасно и етично поведение в мрежата.

Станете приятел с детето си във виртуалния свят- направете регистрация в ползваните/достъпваните от него електронни дискуссионни групи, социалните мрежи, чат програми, които представляват форум за обмен на знания, информация, видеоклипчета, снимки, дискусии, създаване на нови запознанства и др. Това ще ви даде възможност да имате пряк поглед върху поведението на детето ви в мрежата.