

**НАЧАЛНО УЧИЛИЩЕ
„ИЛИЯ РАШКОВ БЛЪСКОВ“
ШУМЕН**



ул. "Христо Смирненски" № 9
директор: 054/861 308
канцелария: 054/862 924
e-mail: info-2700082@edu.mon.bg

УТВЪРДИЛ:

Свилена Димитрова

Директор на НУ "Илия Р. Блъсков"

(Заповед №65/12.10.2026)



ПРАВИЛА
ЗА БЕЗОПАСНОСТ НА УЧЕНИЦИТЕ
В КОМПЮТЪРНАТА МРЕЖА В УЧИЛИЩЕ, В ИНТЕРНЕТ
И ПРИ ИЗПОЛЗВАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ

Правилата са приети с протокол от заседание на Общото събрание №4/18.09.2026 г.

I. ОБЩИ ПОЛОЖЕНИЯ

Настоящите правила уреждат организацията, отговорностите и изискванията за безопасно, отговорно и етично използване на компютърната мрежа на НУ „Илия Рашков Блъсков“, интернет, дигитални платформи, електронни устройства и инструменти с изкуствен интелект от учениците, педагогическите специалисти и родителите.

Правилата се прилагат при използване на училищната мрежа и училищните устройства, както и при учебни дейности с лични устройства, когато това е разрешено от педагогически специалист. Те имат превантивен характер и са насочени към защита на детето, личните данни, достойнството, здравето и сигурността му в дигитална среда.

1. Цели

- да се гарантира достъпът на учениците до подходяща и полезна за възрастта им дигитална информация и образователни ресурси;
- да се предотвратяват рискове, свързани с кибертормоз, измами, фалшиви профили, неподходящо съдържание, зловреден софтуер и злоупотреба с лични данни;
- да се изграждат умения за критично мислене, проверка на информацията и разпознаване на манипулативно, подвеждащо или генерирано съдържание;
- да се определят ясни отговорности на директора, педагогическите специалисти, системния администратор/отговорното лице, учениците и родителите;
- да се осигури своевременна реакция при инцидент в интернет, кибертормоз, заплаха, измама или друг риск за ученик.

2. Основни принципи

- равен и безопасен достъп до цифрови образователни ресурси;
- защита на личния живот, личните данни и достойнството на детето;
- използване на училищната мрежа и устройства предимно за образователни цели;
- съобразяване с възрастта на учениците и условията за ползване на съответните платформи;
- активен педагогически контрол и подкрепа при работа в дигитална среда;
- сътрудничество между училище, родители и компетентни институции при възникнал риск;
- пропорционална реакция, насочена първо към безопасността и подкрепата на детето.

3. Обхват на училищната компютърна мрежа

Училищната компютърна мрежа включва всички свързани по кабелен или безжичен път компютри, лаптопи, таблети, интерактивни дисплеи, принтери, мрежови устройства и други технически средства в сградата на училището, както и лични устройства, когато са свързани към училищната мрежа с разрешение.

В учебно време интернет и училищната мрежа се използват от учениците само за дейности, определени или разрешени от педагогически специалист.

II. ПРАВА НА УЧЕНИЦИТЕ В ДИГИТАЛНА СРЕДА

1. Да използват определените за учебни цели устройства и мрежови ресурси при спазване на настоящите правила.

2. Да получават ясни и разбираеми указания за безопасно поведение в интернет и при работа с изкуствен интелект.
3. Да бъдат информирани кои приложения, сайтове и услуги могат да използват в конкретна учебна дейност.
4. Да получат помощ от учител, класен ръководител, педагогически съветник, директор или родител, когато онлайн съдържание или общуване ги тревожи, плаши или наранява.
5. Да бъдат защитени от унижително отношение, кибертормоз, натиск, изнудване, заплахи и неправомерно разпространяване на техни данни, снимки, аудио или видео.
6. Да не бъдат принуждавани да създават личен профил в услуга, която не е подходяща за възрастта им или не е необходима за учебния процес.

III. ОТГОВОРНОСТИ НА ДИРЕКТОРА И ПЕДАГОГИЧЕСКИТЕ СПЕЦИАЛИСТИ

1. Директорът

- Организира изпълнението на настоящите правила и контролира спазването им.
- Определя отговорно длъжностно лице/лица за техническата поддръжка и сигурността на училищната мрежа.
- Осигурява, в рамките на техническите възможности, мерки за ограничаване на достъпа до вредно, незаконно или неподходящо за възрастта съдържание.
- Организира запознаването на педагогическите специалисти, учениците и родителите с правилата в началото на учебната година и при необходимост след актуализация.
- Организира действията на училището при установен кибертормоз, злоупотреба с лични данни, заплаха, измама или друго рисково онлайн поведение.
- При данни за дете в риск или за престъпление уведомява компетентните органи съобразно характера на случая и действащите процедури за закрила на детето.
- Следи правилата да се съгласуват с Правилника за дейността на училището, механизма за противодействие на тормоза и правилата за защита на личните данни.

2. Педагогическите специалисти

- Разясняват на учениците правилата за безопасно и отговорно поведение в интернет на език, подходящ за възрастта им.
- Наблюдават работата на учениците с училищни устройства и интернет по време на организирана учебна дейност.
- Определят предварително кога и по какъв начин е разрешено използването на интернет и инструменти с изкуствен интелект.
- Не изискват от ученици да предоставят излишни лични данни или да използват платформа в противоречие с възрастовите ѝ изисквания.
- Прекратяват достъпа до вредно, опасно или неподходящо съдържание и уведомяват директора при инцидент.
- Подкрепят ученик, станал обект на кибертормоз или друга онлайн злоупотреба, без обвиняване или публично разгласяване на случая.
- Насърчават проверката на информацията, уважението към авторските права и посочването на използвана помощ от изкуствен интелект, когато това е изисквано в учебната задача.

- Не публикуват снимки, видео, аудио или лични данни на ученици извън утвърдените училищни канали и без наличие на приложимо правно основание/съгласие.

IV. ПРАВА И ОТГОВОРНОСТИ НА РОДИТЕЛИТЕ

1. Родителите имат право

- да получават информация за правилата и за мерките за онлайн безопасност в училището;
- да бъдат информирани своевременно при установен значим инцидент, засягащ тяхното дете, съобразно необходимостта от защита на всички деца в случая;
- да обсъждат с училището подходящи мерки за подкрепа при кибертормоз, злоупотреба с профил, снимка, лични данни или друго рисково онлайн поведение;
- да получават насоки към официални ресурси за онлайн безопасност и закрила на детето.

2. Родителите съдействат, като

- разговарят с детето за безопасно поведение в интернет и за рисковете от общуване с непознати;
- следят възрастовите ограничения на приложенията и социалните платформи и не насърчават заобикалянето им;
- подпомагат детето да използва силни пароли и да не ги споделя с други лица;
- обясняват, че снимка, видео, чат или друга информация, изпратена онлайн, може да бъде копирана и разпространена извън първоначалния контекст;
- следят разумно времето пред екран и баланса между дигитални дейности, движение, сън и общуване;
- уведомяват класния ръководител или директора, когато узнаят, че детето им е обект или участник в кибертормоз, заплаха, измама или друга значима онлайн злоупотреба, свързана с училищната общност.

V. ОБЩИ ПРАВИЛА ЗА БЕЗОПАСНО ПОВЕДЕНИЕ НА УЧЕНИЦИТЕ В ИНТЕРНЕТ

Когато използвам интернет, училищната мрежа или дигитално устройство, спазвам следните правила. Ако не разбирам някое от тях, питам учител или родител.

1. Не споделям адрес, телефон, пароли, кодове за достъп, местоположение, данни за профили, лични документи или друга чувствителна информация за себе си и семейството си.
2. Не съобщавам на непознати къде уча, кога съм сам/сама, кога семейството ми отсъства или други сведения, които могат да бъдат използвани срещу мен.
3. Не изпращам и не публикувам снимки, видео или аудио на себе си без знанието на родител/отговорен възрастен; не публикувам такива материали за други хора без разрешение.
4. Не приемам покани, съобщения, файлове, линкове или видеоразговори от непознати лица.
5. Не се срещам с човек, с когото съм се запознал/а само в интернет. Ако някой предлага среща, веднага казвам на родител или учител.
6. Не използвам чуждо потребителско име, парола, профил или електронна поща.
7. Не се опитвам да разбивам пароли, да заобикалям ограничения, да променям настройки на училищни устройства или да получавам достъп до чужди файлове и профили.

8. Не свалям и не инсталирам програми, игри, приложения, разширения или файлове на училищно устройство без разрешение.
9. Не отварям подозрителни прикачени файлове и линкове, дори когато изглеждат изпратени от познат; при съмнение питам възрастен.
10. Не пиша, споделям или препращам обидни, унизителни, заплашителни, неприлични или злепоставящи съобщения и материали.
11. Не създавам фалшиви профили и не се представям за друг човек.
12. Ако някой ме обижда, заплашва, изнудва или ме кара да се чувствам неудобно, не споря с него, не отмищам и не продължавам разговора. Пазя доказателство и казвам на възрастен.
13. При кибертормоз правя екранна снимка, ако е безопасно, блокирам профила и показвам съдържанието на родител или учител.
14. Не посещавам сайтове и не използвам приложения, които са неподходящи за възрастта ми или са забранени от учителя/училището.
15. Когато приключа работа на общо устройство, излизам от профила си. Ако видя отворен чужд профил, не го разглеждам и уведомявам учителя.
16. Използвам училищната мрежа само за разрешени дейности и се грижа за устройствата.
17. Не вярвам автоматично на всичко, което виждам онлайн. Проверявам информацията с учител, учебник или надежден източник.
18. При съмнение, страх или грешка търся помощ от възрастен. Няма нужда да прикривам проблем, за да го решавам сам/сама.

VI. БЕЗОПАСНО, ОТГОВОРНО И ЕТИЧНО ИЗПОЛЗВАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ

1. Общи правила

- Изкуственият интелект може да създава и обработва текст, изображения, звук, видео и друга информация, но може и да допуска грешки.
- Учениците използват инструменти с изкуствен интелект само когато учителят е разрешил това за конкретна дейност и по начин, подходящ за възрастта им.
- Използването на изкуствен интелект не освобождава ученика от отговорност за съдържанието, което представя, използва или споделя.
- Не се използва услуга, чиито условия не допускат възрастта на ученика, освен ако платформата има специално училищно/детско решение и използването е организирано законосъобразно от училището.

2. Защита на личните данни при използване на ИИ

- Не въвеждам в ИИ своето име, адрес, телефон, пароли, данни за профили, местоположение, снимки на документи или друга лична информация, освен когато учителят е организиран безопасна учебна среда и изрично е обяснил какви данни могат да се използват.
- Не качвам снимки, видеозаписи, аудио, ученически работи или документи, съдържащи лични данни на съученици, учители, родители или други лица.
- Не въвеждам поверителна служебна информация, данни от училищни документи, списъци с ученици, медицинска информация или информация за конкретни семейства.

- Не предоставям пароли, кодове за достъп или данни за вход на система с изкуствен интелект.

3. Надеждност и проверка на информацията

- Помня, че ИИ може да даде неточен, непълен или измислен отговор.
- Проверявам важната информация чрез учебник, учител, официален източник или друг надежден материал.
- Не приемам отговора за верен само защото е написан убедително или подробно.
- Различавам факт от мнение и се замислям дали текст, снимка, видео или звук може да е генериран или манипулиран.

4. Използване на ИИ в учебния процес

- Спазвам указанията на учителя за това дали ИИ е разрешен и за какво може да се използва.
- Когато задачата е за самостоятелно изпълнение, не използвам ИИ вместо собствената си работа.
- Не представям като изцяло свое съдържание, което е създадено в значителна степен от ИИ.
- Когато учителят изисква, посочвам, че съм използвал/а ИИ и как – например за идеи, редактиране, обяснение, проверка или превод.
- ИИ не замества четенето, мисленето, ученето, творчеството и общуването с учителя и съучениците.
- Не използвам ИИ за създаване на обидни, унизителни, заплашителни, дискриминационни или подвеждащи материали.
- Не използвам ИИ за фалшиви профили, фалшиви снимки, видео или аудио с цел да осмее, измама, злепоставя или тормозя друг човек.
- Не използвам ИИ за заобикаляне на училищни правила, измама, неправомерен достъп до чужди профили, устройства или информация.

VII. ПРАВИЛА ЗА СИГУРНОСТ НА УЧИЛИЩНИТЕ УСТРОЙСТВА И ПРОФИЛИ

1. Училищните устройства се използват внимателно и само по предназначение.
2. Не се променят настройки, мрежови конфигурации, профили, защитни програми или филтри без разрешение.
3. Не се включват непроверени външни носители и устройства.
4. Паролите за училищни профили са лични и не се споделят между ученици.
5. При съмнение, че парола е станала известна на друг човек, ученикът съобщава на учител/отговорно лице и паролата се сменя.
6. Учениците не използват администраторски акаунти и не се опитват да получат разширени права за достъп.
7. При съобщение за вирус, измама, фалшив прозорец за вход, подозрително изтегляне или необичайно поведение на устройството ученикът прекратява действието и уведомява учителя.
8. След приключване на работа се затварят отворените профили и се оставя устройството в състояние, определено от учителя.

VIII. ДЕЙСТВИЯ ПРИ КИБЕРТОРМОЗ, ЗАПЛАХА ИЛИ ДРУГ ОНЛАЙН ИНЦИДЕНТ

1. Действия на ученика

- Прекратява общуването и не отговаря с обида, заплаха или отмъщение.
- Не изтрива прибързано доказателства; ако е безопасно, прави екранна снимка на съобщението, профила или публикацията.
- Блокира профила/контакта, когато това е възможно.
- Незабавно уведомява родител, класен ръководител, учител, педагогически съветник или директор.
- При непосредствена опасност за живота или здравето се търси помощ от възрастен и при необходимост се подава сигнал на 112.

2. Действия на училището

- Осигурява безопасност и подкрепа на засегнатото дете и прекратява достъпа до рисковото съдържание в училищната среда, когато е възможно.
- Установява основните факти без публично разпитване или унижаване на участващите деца.
- Уведомява родителите на засегнатите ученици по подходящ и законосъобразен начин.
- Прилага действащия в училището механизъм за превенция и противодействие на тормоза, когато случаят представлява тормоз между ученици.
- При данни за дете в риск уведомява компетентните органи по закрила на детето; при данни за престъпление или непосредствена опасност се уведомяват компетентните органи на МВР.
- Съхранява наличните доказателства и ограничава достъпа до тях до лицата, които имат служебна необходимост.
- Планира последващи мерки за подкрепа и превенция, включително работа с класа, когато това е необходимо и не води до допълнително разкриване на лични данни.

3. Алгоритъм за уведомяване

1. Ученикът установява проблем	Съобщава на родител и/или учител, класен ръководител, педагогически съветник, директор.
2. Училището получава сигнал	Осигурява безопасност, запазва наличните доказателства и уведомява директора.
3. Оценка на риска	Преценява се дали има кибертормоз, заплаха, сексуална експлоатация, измама, пробив в сигурността или друг риск.
4. Външно уведомяване при необходимост	ДСП/Отдел „Закрила на детето“, МВР/ГДБОП, 112 при непосредствена опасност, Национален център за безопасен интернет.
5. Последващи действия	Информиране и подкрепа на семейството, мерки в училище, проследяване и превенция на повторение.

IX. ПОЛЕЗНИ КОНТАКТИ ПРИ РИСК В ДИГИТАЛНА СРЕДА

Ресурс	Контакт / предназначение
Национална телефонна линия за деца	116 111 – безплатна и денонощна.
Национален център за безопасен интернет – SafeNet	safenet.bg; консултативна линия 124 123; онлайн чат и форма за сигнал.
ГДБОП – Киберпрестъпност	cybercrime.bg – информация и канали за сигнализиране при киберпрестъпления.
Единен европейски номер за спешни повиквания	112 – при непосредствена опасност за живота, здравето или сигурността.
Органи за закрила на детето	Дирекция „Социално подпомагане“/Отдел „Закрила на детето“ по настоящ адрес на детето.

Х. КРАТЪК РЕЧНИК ЗА УЧЕНИЦИ И РОДИТЕЛИ

Кибертормоз: Повтарящо се или значимо поведение в дигитална среда, което унижава, плаши, заплашва, изолира или вреди на друг човек чрез съобщения, публикации, снимки, видео, фалшиви профили и други онлайн средства.

Фишинг: Измама, при която съобщение, сайт или профил се представя за надежден и се опитва да получи парола, код, лични или финансови данни.

Фалшив профил: Профил, създаден с чуждо име, снимка или измислена самоличност с цел подвеждане.

Зловреден софтуер: Програма или файл, който може да увреди устройство, да открадне данни или да даде неразрешен достъп.

Лични данни: Информация, чрез която човек може да бъде разпознат пряко или косвено – например име, снимка, адрес, телефон, местоположение, идентификатор, данни за профил.

Дийпфейк/синтетично съдържание: Изображение, видео или звук, създаден или променен с технологии, включително ИИ, така че да изглежда като реално събитие или изказване.

Цифров отпечатък: Следите, които остават от действията ни онлайн – публикации, коментари, снимки, регистрации, търсения и други.

Двуфакторна защита: Допълнителна стъпка при вход в профил – например код от приложение или съобщение, освен паролата.

ХІ. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Настоящите правила са задължителни за учениците при използване на училищната компютърна мрежа, училищни устройства и разрешени дигитални платформи.
2. Класните ръководители запознават учениците с правилата в началото на учебната година по начин, съобразен с възрастта им, а родителите се информират чрез утвърдените канали на училището.
3. Правилата се публикуват на интернет страницата на училището и се предоставят на разположение на педагогическите специалисти и родителите.

4. При промяна на нормативни изисквания, технологични рискове или организацията на училището правилата се актуализират.
5. За неуредените в настоящия документ случаи се прилагат действащото законодателство, вътрешните правила на училището, правилата за защита на личните данни и механизмите за закрила на детето и противодействие на насилието и тормоза.

НУ „Илия Рашков Блъсков“ – гр. Шумен