СРЕДНО УЧИЛИЩЕ „КОНСТАНТИН КОНСТАНТИНОВ“ - СЛИВЕН

УТВЪРДИЛ: /п/
Весела Паскалева
Директор на СУ „К. Константинов“ – Сливен
Утвърдени със Заповед №РД-06-1669/14.09.2026 г.

ПРАВИЛА
ЗА СИГУРНОСТ И БЕЗОПАСНОСТ
НА УЧЕНИЦИТЕ В ИНТЕРНЕТ
за учебната 2026/2027 година

I. ЦЕЛИ И ОСНОВНИ ПРИНЦИПИ

А. Цели

Правилата имат за цел:

1. Да гарантират правото на учениците на достъп до подходяща информация и материали в мрежата.
2. Да осъществят превенция и да синтезират на едно място информацията за опасностите в интернет.
3. Да предоставят конкретни насоки за закрила на детето и безопасно поведение в компютърната мрежа в училище и в интернет.
4. Да подобрят координацията и отговорностите на всички заинтересовани страни.

Б. Основни Принципи

Основните принципи за работа в компютърната мрежа в училище и в интернет са:

1. Равен достъп на всички ученици.
2. Защита на учениците от вредно или незаконно съдържание (самонараняване, наркотици, хазарт, анорексия, порнография, насилие, тероризъм, етническа/религиозна нетолерантност, самоубийство и др.).
3. Зачитане и защита на личната неприкосновеност и личните данни.
4. Подготовка и контрол на учениците за безопасно и отговорно поведение онлайн.
5. Сътрудничество в дух на толерантност и добронамереност между училището и родителите/настойниците.

В. Обхват

- Компютърната мрежа в училище се използва в учебни часове **само за образователни цели**.
- Обхватът включва всички устройства (компютри, смартфони, лаптопи и таблети) с безжичен достъп до интернет, ситуирани в кабинетите, класните стаи и административните помещения на институцията.

II. ОТГОВОРНОСТИ НА УЧАСТНИЦИТЕ В ОБРАЗОВАТЕЛНИЯ ПРОЦЕС

1. Директор на училището

Директорът е длъжен да:

- Организира дейността по изпълнението на тези правила и осигурява достъп до мрежата, ефективен контрол и защита от вредно или незаконно съдържание.
- Осигурява, при техническа възможност, проследяване на трафика, осъществяван чрез мрежата на училището.
- **При констатиране на кибертормоз или незаконно съдържание/поведение** в мрежата, уведомява незабавно компетентните органи (Дирекция „Социално подпомагане“ и Главна дирекция „Борба с организираната престъпност“, отдел „Киберпрестъпност“ на МВР). Оказва съдействие на компетентните органи.
- Организира в началото на всяка учебна година запознаване на учениците и родителите/настойниците с правилата за безопасна работа в мрежата.
- Осигурява отговорно лице за изпълнение на функциите на **Системен администратор**.

2. Педагогически специалисти

Педагогическите специалисти са длъжни да:

- Разясняват правилата за безопасно и отговорно поведение при работа в мрежата и в интернет.
- Осъществяват постоянно наблюдение и контрол върху работата на учениците в мрежата в учебно време.
- Предприемат незабавни мерки за преустановяване на достъпа до незаконно и вредно съдържание.
- Уведомяват незабавно Директора при нарушаване на правилата, случаи на кибертормоз или установяване на незаконно съдържание/поведение.
- Оказват подкрепа на ученици, обект на кибертормоз, чрез първоначална психологическа подкрепа.

3. Системен администратор

Системният администратор:

- Осигурява общата безопасност и функционалност на мрежата.
- Предлага и прилага мерки, ограничаващи достъпа до вредно или незаконно съдържание и поведение в интернет.
- Следи трафика и извършва периодичен преглед на мрежата за заплахи и рискове.
- Уведомява незабавно Директора при случаи на кибертормоз или нарушаване на правилата.

4. Родители/Настойници

Родителите/настойниците:

- Носят отговорност да помогнат на детето си да изгради умения за онлайн общуване и безопасно използване на интернет.
- Осъществяват постоянен контрол за сигурността на детето си в интернет и проявяват интерес към активността му в мрежата.
- При установяване, че детето им е жертва на кибертормоз, уведомяват Директора на училището и могат да сигнализират на компетентните органи (ГДБОП, Центъра за безопасен интернет).
- Следят времето за използване на интернет с цел съхраняване здравето на детето.

III. ПРАВА И ЗАДЪЛЖЕНИЯ НА УЧЕНИЦИТЕ

А. Права на учениците

1. Равен достъп до мрежата на образователната институция (с изключение на компютрите в административните помещения).
2. Работа с устройствата в мрежата с подкрепата на педагогически специалист.
3. Обучение за безопасно и отговорно поведение в мрежата и в интернет.
4. Сигурна цифрова среда в училището.
5. Ползване на мобилните си устройства извън учебния процес (почивките), а в учебен час – само при изрично указание на учител за целите на учебния процес.

Б. Задължения на учениците (Правила за безопасност)

Група Правила	Правило
Лична Информация	**1. Не дават лична информация** (адрес, парола, личен телефонен номер) на непознати онлайн.
	2. Не дават информация за местоработата или личен/служебен телефонен номер на родителите, близките или съучениците си **без тяхно разрешение**.
Снимки и Видео	**3. Не изпращат и не качват онлайн свои снимки и видеа** без обсъждане и решение с родителите им.
	4. Не изпращат и не качват онлайн снимки и видеа на други хора (приятели, учители, роднини) без тяхно съгласие.
Онлайн Общуване	**5. Не отговарят на писма и не отварят прикачени файлове, получени от непознат подател**.
	6. Не отговарят на съобщения, които са обидни, заплашителни, неприлични или ги карат да се чувстват неудобно. Информират възрастен.
	7. Ако някой ги обижда или тормози онлайн, не отговарят. Докладват го на отговорен възрастен (родител, учител, педагогически съветник).
	8. Не трябва да приемат срещи с лица, с които са се запознали в интернет, освен след съгласието на родителите им и в тяхно присъствие.
Техническа Сигурност	**9. Не използват чуждо потребителско име, парола и електронна поща**.

Група Правила	Правило
	10. Съветват се с родителите си/учител, преди да свалят или инсталират нова програма/приложение.
	11. Използват трудни и различни за всеки сайт пароли (дълги, с главни и малки букви, цифри и специални знаци).
Докладване на Проблеми	**12. Незабавно информират възрастен** (родител, учител, директор), когато попаднат на материали, които ги карат да се чувстват неудобно или на материали с вредно/незаконно съдържание.
	13. При кибертормоз, правят веднага екранна снимка (скрийншот) на разговора/съдържанието като електронно доказателство, което се предава на отговорен възрастен.

IV. ДОПЪЛНИТЕЛНИ ДОБРИ ПРАКТИКИ И ПРЕПОРЪКИ

А. Управление на профили и лични данни

1. **Настройки за поверителност:** Винаги използвайте настройките за безопасност и защита на личните данни, предлагани от социалните мрежи. Настройте профилите си да бъдат видими **само за приятели**.
2. **Геолокация (Location Sharing):** Изключвайте функцията за геолокация (споделяне на местоположение) на мобилните си устройства и приложения, когато не е необходима, за да не разкривате къде се намирате.
3. **Digital Footprint (Цифрова следа):** Помнете, че всичко, което публикувате онлайн, остава завинаги. Бъдете отговорни за съдържанието, което създавате и споделяте.
4. **Случаи на общи компютри:** Ако ползвате общи компютри (в училище или интернет клуб), винаги проверявайте дали сте излезли от профила си след края на работата.

Б. Защита от зловреден софтуер и измами

1. **Актуализации и Антивирусна програма:** Използвайте антивирусна програма и я обновявайте редовно. Поддържайте последните актуализирани версии на всички програми, тъй като те съдържат кръпки за сигурност.
2. **Критично мислене:** Разпознавайте измамни съобщения, като тези за "печалба от лотария" или фалшиви сигнали, които изискват да дадете лична информация. **Ако нещо звучи твърде хубаво, за да е истина, вероятно е измама.**
3. **Фишинг (Phishing):** Внимавайте с имейли, които Ви карат да дадете пароли или банкови данни. Легитимните компании никога не биха поискали такава информация по имейл.

В. Поведенчески етикет (Netiquette)

1. **Уважение:** Винаги бъдете учтиви и уважителни в онлайн комуникацията. Избягвайте използването на главни букви, тъй като в интернет това се приема за "крещене".

2. **Авторско право:** Не копирайте и не разпространявайте материали (текстове, изображения, музика), защитени с авторско право, без разрешението на автора. Учете се да цитирате и да посочвате източника на информацията.
3. **Достоверност на информацията:** Бъдете критични към информацията, която намирате онлайн. Проверявайте източниците и сравнявайте информацията от различни надеждни сайтове.

V. КОНТАКТИ ЗА ПОМОЩ И ДОКЛАДВАНЕ

Ако попаднете на информация, която не Ви харесва, или сте жертва на кибертормоз, можете да се обърнете за помощ към:

1. **Национална телефонна линия за деца: 116 111** (денонощно и безплатно).
2. **Център за безопасен интернет:** www.safenet.bg (тел. **124 123**).
3. **Отдел „Киберпрестъпност“ към ГДБОП:** http://www.cybercrime.bg/bg
4. **Училищен психолог/Педагогически съветник** (име, ако имате утвърдено лице).
5. **Класния ръководител** или всеки друг учител, на когото имате доверие.