



УТВЪРДЕНА:

Заповед № РД 09-51/ 15.09.2026 г.

.....
(подпис и печат)

Бистра Бойчева.

(име и фамилия на директора)

ИНСТРУКЦИЯ

за безопасно поведение и работа на учениците в интернет среда

I. ОБЩИ РАЗПОРЕДБИ ЗА ДОСТЪП ДО МРЕЖАТА

1. Училищната интернет мрежа (Wi-Fi и кабелна връзка) се използва единствено за образователни цели и дейности, свързани с учебния процес.
2. Забранява се заобикалянето на филтрите за сигурност, инсталирането на VPN програми или прокси сървъри с цел достъп до блокирани от училищната система сайтове.

II. ПРАВИЛА ЗА КИБЕРСИГУРНОСТ И ЛИЧНИ ДАННИ

1. Защита на самоличността: Учениците не трябва да споделят в интернет пространството (социални мрежи, блогове, чатове) свои лични данни – три имена, ЕГН, домашен адрес, телефонен номер, както и лична информация за свои съученици или учители.
2. Сигурност на профилите: Забранява се споделянето на пароли за достъп до училищни платформи (напр. НЕИСП, MS Teams, Google Workspace) с други лица, включително с най-близки приятели.
3. Непознати контакти: Забранява се приемането на покани за приятелство или комуникацията с непознати лица в мрежата, които изискват изпращане на снимки, лична информация или предлагат лични срещи извън училището.

III. ПРАВИЛА ЗА ПОВЕДЕНИЕ И ПРЕДОТВРАТЯВАНЕ НА КИБЕРТОРМОЗ (CYBERBULLYING)

1. Недопускане на агресия: Забранява се използването на училищния интернет за изпращане на обидни, заплашителни, подигравателни или унижаващи съобщения.
2. Защита на личното пространство: Забранява се заснемането на ученици или учители в сградата на училището и последващото публикуване на снимки или видеоклипове в интернет без тяхното изрично устно или писмено съгласие.
3. Училищен етикет: Всички електронни писма, коментари и публикации от училищни профили трябва да спазват добрия тон и правилата на правописа и правоговора.

IV. ЗАБРАНЕНИ ДЕЙНОСТИ В МРЕЖАТА

1. Забранява се достъпът до уебсайтове с порнографско съдържание, хазартни игри, онлайн залагания, сайтове, подтикващи към насилие, расова или религиозна омраза, или употреба на забранени субстанции.
2. Забранява се изтеглянето на пиратски софтуер, филми, музика или торенти чрез училищната мрежа, тъй като това застрашава системата от заразяване с компютърни вируси.

V. АЛГОРИТЪМ НА ДЕЙСТВИЕ ПРИ ВЪЗНИКВАНЕ НА РИСК

1. Ако ученик случайно попадне на сайт с неподходящо или стряскащо съдържание, той трябва незабавно да затвори прозореца и да уведоми преподавателя.

2. При получаване на обидни съобщения или заплахи (кибертормоз), ученикът не трябва да отговаря на тях, а веднага да направи екранна снимка (скрийншот) и да докладва на класния ръководител или на родител.
3. При съмнение за компрометирана парола или хакнат профил, ученикът е длъжен незабавно да съобщи на учителя по Информационни технологии за промяна на данните.