

ПРИЛОЖЕНИЕ №1
КЪМ ЕТИЧНИЯ КОДЕКС НА УЧИЛИЩНАТА ОБЩНОСТ в ПГМЕЕ
гр. Бургас
ПРАВИЛА ЗА КИБЕРБЕЗОПАСНОСТ, ЕТИЧНО ПОВЕДЕНИЕ И ЗАЩИТА В
ЦИФРОВАТА СРЕДА

Настоящите правила са неразделна част от Етичния кодекс на училището и са задължителни за спазване от всички членове на училищната общност (ученици, учители, служители и родители). Тяхната цел е да гарантират безопасна, колегиална и защитена образователна и социална среда в дигиталното пространство.

РАЗДЕЛ I. ОПАЗВАНЕ НА ЛИЧНАТА ИНФОРМАЦИЯ И ПОВЕРИТЕЛНОСТТА

Член 1. Конфиденциалност на личните данни

- (1) Всеки член на училищната общност е длъжен да пази и да не разкрива пред трети лица в интернет лична информация, включително: трите си имена, домашен адрес, пароли за електронни пощи и профили в социалните мрежи, личен телефонен номер и наименованието на училището.
- (2) Категорично се забранява споделянето на информация относно местоработата, служебните или личните телефонни номера на родители, настойници, близки, приятели, съученици и познати без тяхното предварително и изрично разрешение.

Член 2. Публикуване на визуално и мултимедийно съдържание

- (1) Не се допуска изпращането или публикуването онлайн на собствени снимки и видеоклипове, преди това да бъде обсъдено и съгласувано с родителите или лицата, които полагат грижи за ученика.
- (2) Изпращането и качването на снимки и видеоклипове на приятели, съученици, роднини, учители или близки изисква предварително обсъждане с тях. Когато се касае за непълнолетни лица (приятели и съученици), съдържанието трябва да бъде предварително съгласувано и от техните родители, настойници или учители. При тези случаи се попълва декларация за информирано съгласие.

Член 3. Безопасност при онлайн запознанства и срещи

- (1) При общуване в чат платформите трябва да се има предвид, че потребителите онлайн не винаги са тези, за които се представят, и могат да използват подвеждаща информация с цел злоупотреба.
- (2) Препоръчва се винаги да се прави опит за проверка на самоличността на онлайн събеседника чрез проверка на име, имейл, снимка или чрез поставяне на контролен въпрос, на който само истинският човек би знаел отговора. При съмнения трябва да се потърси съвет през сайта на Центъра за безопасен интернет.

РАЗДЕЛ II. ЕТИЧНИ НОРМИ И ПРЕВЕНЦИЯ НА КИБЕРТОРМОЗА

Член 4. Принципи на нетолерантност към вреди и злоупотреби

(1) Действията на членовете на училищната общност в интернет не трябва да вредят на други хора или да противоречат на законите и установените обществени правила.

Член 5. Забрана за кражба на идентичност и нерегламентиран достъп

(1) Използването на чужди потребителски имена, пароли и електронни пощи е абсолютно забранено.

(2) При работа на общи или училищни компютри всеки е длъжен да проверява и да излиза от личния си профил след приключване на работа.

(3) В случай на намиране на устройство, на което друг ученик е оставил профила си отворен, намерилият го е длъжен незабавно да излезе от профила, без да преглежда, променя, изтрива или добавя информация в него.

Член 6. Забрана за тормоз, обиди и дезинформация

(1) Забранява се писането, публикуването и разпространяването на съдържание, което е обидно, заплашително, унижително или злепоставящо за когото и да било.

(2) Публикуването на невярна и изопачена информация за друг човек — дори когато е представено под формата на шега — е нарушение на етичните норми, тъй като може да причини неприятни преживявания и да доведе до сериозни злоупотреби с потърпевшия.

Член 7. Опазване на престижа и доброто име на училището

(1) Забранява се публикуването и разпространяването в интернет пространството на материали (включително текстове, коментари, снимки, видеоклипове и колажи), които уронват престижа, авторитета и доброто име на училището или на членовете на училищната общност (ученици, учители, служители и училищно ръководство).

(2) Публикуването на обидни, злепоставящи, неверни или изопачени твърдения по адрес на училището или негови представители се счита за грубо нарушение на етичните норми. Всички действия в цифрова среда са проследими и могат да нанесат трайни вреди на училищната институция или на група хора, принадлежащи към нея.

РАЗДЕЛ III. ТЕХНИЧЕСКА ЗАЩИТА НА ИНФОРМАЦИОННИТЕ СРЕДСТВА

Член 7 (втори). Защита от зловреден софтуер

(1) Забранява се отварянето на прикачени файлове и отговарянето на електронни писма, получени от непознати податели, поради риск от заразяване на устройствата със зловреден софтуер и вируси, които могат да ги увредят или да ги направят достъпни за външен злонамерен достъп.

(2) Свалянето и инсталирането на нови програми и приложения на служебни компютри, телефони трябва да се извършва само след консултация и одобрение от учител.

Член 8. Настройки за сигурност и хигиена на сърфиране

- (1) Всички потребители трябва активно да използват настройките за безопасност и защита на личните данни в социалните мрежи, мобилните приложения и браузърите.
- (2) Задължително е използването на функцията за безопасно сърфиране и избягването на интернет сайтове, чието съдържание е неподходящо за съответната възрастова група.
- (3) Достъпът до цифрови платформи трябва да се защитава чрез трудни пароли (дълги, съдържащи комбинация от главни и малки букви, цифри и специални знаци), като за всеки отделен сайт се използва различна парола.
- (4) Заедно с родителите или учителите трябва да се поддържат най-новите актуализирани версии на програмите, приложенията и да се използва редовно обновявана антивирусна програма.

РАЗДЕЛ IV. РЕАКЦИЯ, СИГНАЛИЗИРАНЕ И ПАРТНЬОРСТВО ПРИ ПРОБЛЕМИ В МРЕЖАТА

Член 9. Действия при получаване на обидни съобщения и кибертормоз

- (1) В случай на получаване на обидни, заплашителни или неприлични съобщения, ученикът не трябва да отговаря на тях, за да се избегнат по-големи вреди.
- (2) Профилът на лицето, извършващо тормоза, трябва незабавно да бъде блокиран в съответната платформа.
- (3) Потърпевшият или свидетелят на тормоза трябва незабавно да информира доверен възрастен — родител, класен ръководител, учител, директор или педагогически съветник.
- (4) Задължително е незабавното правене на екранна снимка (скрийншот) на съответния разговор, снимка или видеосъобщение като електронно доказателство за тормоза.

Член 10. Сигнализиране за незаконно и вредно съдържание

- (1) При попадане на материали в интернет, които предизвикват неудобство и страх, или съдържат вредно и незаконно съдържание (като порнография, проповядване на насилие и тероризъм, етническа и религиозна нетолерантност, разпространение на наркотици, хазарт и др.), учениците са длъжни незабавно да съобщят на родител, учител, директор или педагогически съветник.
- (2) Сигнали за вредно съдържание или кибертормоз могат да се подават и самостоятелно директно към администраторите на съответните уебсайтове.

Член 11. Официални национални канали за помощ и сигнализиране

- (1) При необходимост от консултация, подкрепа или спешно подаване на сигнали за киберпрестъпления, училищната общност използва следните легитимни платформи и контакти:

№	Институция / Организация	Контакт / Платформа	Предназначение
1	Държавна агенция за закрила на детето (ДАЗД)	Тел. 116 111	Национална телефонна линия за деца (денонощна, безплатна)

2	Център за безопасен интернет	Тел. 124 123 www.safenet.bg	Консултация, подкрепа и онлайн чат-модул за сигнали
3	ГДБОП – МВР Отдел "Киберпрестъпност"	www.cybercrime.bg	Официална форма за сигнализиране на киберпрестъпления
4	ГДБОП (Главна дирекция)	www.gdbop.bg	Допълнителна уеб платформа за сигурност
5	Асоциация "Деметра" Проект "Спаси дете"	www.spasidete.com	Превенция и защита на деца в риск
6	ГДБОП Киберсигурност	Facebook страница: bgcybercrime	Официален канал на МВР в социалните мрежи за сигнали