



ВЪТРЕШНИ ПРАВИЛА

ЗА РАБОТА С ОБЛАЧНАТА ПЛАТФОРМА GOOGLE WORKSPACE FOR EDUCATION

В ЧСЕУ „Д-Р МАРИЯ МОНТЕСОРИ“ – ГР. БУРГАС

*Приети на заседание на ПС с протокол № 10 от 11.09.2026 г. и утвърдени със заповед
на директора № от 14.09.2026 г.*



I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Предмет и обхват

(1) Настоящите правила уреждат реда, условията и изискванията за използване на училищния дигитален домейн и на облачната платформа Google Workspace for Education в Частно средно езиково училище „Д-р Мария Монтесори“ – гр. Бургас, наричано по-нататък „Училището“.

(2) Правилата се прилагат за:

1. учениците;
2. учителите;
3. директора и останалите членове на ръководството;
4. административния и помощния персонал;
5. системните администратори;
6. други лица, на които Училището е предоставило временен или постоянен профил в училищния домейн.

(3) Google Workspace for Education е официална, управлявана от Училището облачна среда, предназначена за обучение, комуникация, сътрудничество, създаване и съхраняване на учебно съдържание, организация на учебния процес и изпълнение на служебни задължения.

(4) Училищният профил не е личен профил. Той се създава, конфигурира и управлява от Училището и се предоставя на потребителя единствено за периода, през който същият е ученик, служител или друго оправомощено лице.

(5) Училището управлява профилите, правата за достъп, активираните услуги и настройките за сигурност. Това не означава, че Училището придобива авторските

права върху всички произведения, разработки и материали, създадени от потребителите. Авторските и сродните права се уреждат съгласно действащото законодателство.



Чл. 2. Google Workspace for Education

(1) Google Workspace for Education представлява съвкупност от облачни услуги за комуникация, създаване на съдържание, съвместна работа, обучение, управление и защита на информацията.

(2) Услугите, достъпни чрез училищния профил, се разделят на:

1. Основни услуги на Google Workspace for Education;
2. други услуги на Google Workspace for Education;
3. Допълнителни услуги на Google;
4. приложения и услуги на трети страни.

(3) Достъпът до определена услуга не възниква автоматично със създаването на профила. Директорът и Системният администратор определят кои услуги се активират за отделните организационни единици, класове, възрастови групи и категории потребители.

Чл. 3. Основни услуги

(1) Основните услуги са услуги, предоставяни по силата на договора за Google Workspace for Education и приложимите условия за обработване и защита на данните (https://workspace.google.com/intl/en/terms/user_features/).

(2) Посочването на Gemini for Education и NotebookLM като Основни услуги не означава автоматично, че те са достъпни за всички ученици. Достъпът до тях се определя според:

1. възрастта на учениците;
2. актуалните технически и възрастови ограничения на услугата;
3. настройките в Google Admin Console;
4. решението на Училището;
5. вътрешните правила на Училището за отговорно използване на изкуствен интелект.



(3) За ученици, за които дадена услуга не е подходяща или не е разрешена, Системният администратор я деактивира или ограничава на ниво организационна единица или група.

Чл. 4. Други и допълнителни услуги

(1) Към другите услуги на Google Workspace for Education могат да се отнасят AppSheet, Read Along и други услуги, определени от Google в актуалното обобщение на услугите.

(2) Допълнителните услуги са потребителски услуги на Google, които не са част от Основните услуги, но могат да бъдат достъпни чрез училищен профил (https://knowledge.workspace.google.com/admin/users/advanced/turn-on-or-off-additional-google-services?hl=en#additional_google_services)

(3) Допълнителните услуги не се активират автоматично за учениците.

(4) Допълнителна услуга може да бъде разрешена само когато:

1. има ясна образователна цел;
2. използването ѝ е съобразено с възрастта на учениците;
3. извършена е преценка на необходимостта и рисковете;
4. директорът или упълномощено от него лице е одобрил използването;
5. Системният администратор е извършил необходимите настройки;
6. е предоставена информация на родителите;
7. е получено родителско или настойническо съгласие, когато такова се изисква.

(5) За ученици под 18 години Допълнителни услуги се активират само след изпълнение на приложимите изисквания за родителско или настойническо съгласие.

6) За образователни цели Училището разрешава за използване от учениците следните Допълнителни услуги на Google: YouTube, Applied Digital Skills, Google Maps, Google Earth, Google Translate, Google Arts & Culture, Google Books, Search and Assistant, CS First и Socratic. Достъпът до всяка услуга се предоставя съобразно възрастовите



ограничения и функционалните ограничения, определени от Google, както и с административните настройки на Училището.

(7) Училището може впоследствие да разреши и други Допълнителни услуги на Google, когато са подходящи за съответната възрастова група, имат конкретна образователна цел и са одобрени от ръководството след педагогическа, техническа и организационна преценка. Преди активирането им за ученици под 18 години родителите/настойниците се информират и се получава необходимото съгласие съгласно условията на Google и приложимото законодателство.

Чл. 5. Приложения на трети страни

(1) „Приложение на трета страна“ е всяко приложение, уебсайт или цифрова платформа, която не се предоставя като Основна услуга по договора за Google Workspace for Education.

(2) Забранява се самоволното използване на училищния профил за:

1. регистрация в непроверени външни платформи;
2. предоставяне на достъп чрез „Sign in with Google“;
3. инсталиране на приложения от Google Workspace Marketplace;
4. предоставяне на външно приложение на достъп до Gmail, Drive, Calendar, Contacts или други училищни данни.

(3) Приложение на трета страна може да се използва само след предварително одобрение от Системния администратор и от ръководството на Училището.

(4) Преди одобряването се проверяват най-малко:

1. целта на приложението;
2. видовете данни, до които иска достъп;
3. условията за използване;
4. политиката за поверителност;
5. местата и сроковете за съхраняване на данните;
6. възможността за изтриване на профила и данните;



7. наличието на реклами;
8. възрастовите ограничения;
9. необходимостта от родителско съгласие.

II. ЗАЩИТА И ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 6. Администратор и обработване на данните

(1) Училището определя целите, категориите потребители, начина на използване и административните настройки на училищния домейн и е администратор на лични данни за извършваните от него дейности по обработване.

(2) По отношение на клиентските данни в Основните услуги Google обработва информацията съгласно договора за Google Workspace for Education, приложимото споразумение за обработване на данни и документираните указания на Училището.

(3) Обработването се извършва при спазване на:

1. Регламент (ЕС) 2016/679 – Общ регламент относно защитата на данните;
2. Закона за защита на личните данни;
3. Закона за предучилищното и училищното образование;
4. приложимите подзаконови нормативни актове;
5. вътрешните правила на Училището за защита на личните данни;
6. договорните условия за Google Workspace for Education.

(4) В зависимост от конкретната дейност правното основание за обработване може да бъде:

1. изпълнение на договор;
2. изпълнение на законово задължение;
3. изпълнение на задача, свързана с образователната дейност;
4. защита на легитимен интерес на Училището, когато правата и интересите на детето не имат преимущество;



-
5. изрично съгласие, когато услугата или дейността е доброволна и съгласието се изисква.

(5) Когато обработването на данни на лице под 14 години се основава на съгласие, съгласието се предоставя от родителя, който упражнява родителските права, или от настойника.

Чл. 7. Категории обработвани данни

(1) При създаване и използване на училищен профил могат да се обработват:

1. име и фамилия;
2. училищен електронен адрес;
3. клас, паралелка или организационна единица;
4. длъжност или служебна роля;
5. профилна снимка, когато е разрешена;
6. данни за удостоверяване и защита на профила;
7. учебни задания, текстове, презентации, таблици, изображения, аудио- и видеоматериали;
8. оценки, обратна връзка и коментари, когато се обработват в Classroom или друга разрешена услуга;
9. електронни писма и служебна комуникация;
10. данни за споделяне и съвместна работа;
11. технически данни и данни за активност.

(2) Техническите данни могат да включват:

1. IP адрес;
2. вид на устройството;
3. браузър и операционна система;
4. дата и час на влизане;
5. приблизително местоположение, изведено от IP адрес или от настройките на устройството;
6. системна активност;
7. използвани услуги;
8. данни за грешки и сигурност;



9. история на административни действия.

(3) В училищния профил не се въвеждат повече лични данни, отколкото са необходими за конкретната учебна или служебна цел.

(4) Единен граждански номер, данни от лични документи, медицинска информация, данни за семейното положение, финансови данни и други чувствителни или поверителни данни не се въвеждат в общодостъпни, публично споделени или незащитени файлове.

Чл. 8. Видимост и достъп до данните

(1) Информацията, създадена или съхранявана в училищния профил, не е автоматично публична.

(2) В зависимост от настройките и начина на споделяне информацията може да бъде достъпна за:

1. самия потребител;
2. конкретни ученици и учители;
3. участниците в съответния курс в Google Classroom;
4. членовете на определена група или организационна единица;
5. служители, на които е предоставен служебен достъп;
6. Системния администратор, само в рамките на административните му правомощия;
7. Google и негови одобрени подизпълнители, доколкото това е необходимо за предоставяне, защита и поддръжка на услугите;
8. трети лица, само когато потребителят или Училището изрично са споделили информацията с тях и това е разрешено.

(3) Съдържанието може да стане публично достъпно, когато потребителят го публикува или сподели с настройка „Всеки с връзката“ или „Публично“, ако такава настройка е разрешена.



(4) Публичното споделяне от ученически профили е забранено, освен когато е част от предварително одобрена учебна дейност и е извършено под ръководството на учител.

(5) Учителите са длъжни предварително да проверяват настройките за споделяне на файлове, папки, сайтове, видеоматериали, формуляри и електронни таблици.

Чл. 9. Реклами и използване на информацията

(1) В Основните услуги на Google Workspace for Education не се показват реклами.

(2) Личната информация, събрана при използване на Основните услуги, не се използва за рекламни цели.

(3) При някои Допълнителни услуги е възможно показване на реклами, но за профили на ученици в начални и средни училища информацията от училищния профил и предходната активност не следва да се използват за персонализиране и насочване на рекламите.

(4) Независимо от ал. 3 Училището активира Допълнителни услуги само след конкретна преценка на тяхната образователна необходимост и въздействие върху правата на учениците.

Чл. 10. Права на учениците и родителите

(1) Учениците и техните родители или настойници имат право да получат информация относно:

1. целите на обработването;
2. категориите обработвани данни;
3. активираните услуги;
4. лицата и категориите получатели;
5. сроковете за съхраняване;
6. начина за упражняване на правата им;
7. възможността за оттегляне на дадено съгласие.



(2) Искания за достъп, коригиране, ограничаване или изтриване на лични данни се подават до директора на Училището или до определеното длъжностно лице по защита на данните.

(3) Правото на изтриване не се прилага, когато Училището е длъжно да съхранява информацията по закон, за защита на права и законни интереси или за установяване на факти при нарушение.

(4) Оттеглянето на съгласие за Допълнителна услуга не засяга законосъобразността на обработването преди оттеглянето.

III. СЪЗДАВАНЕ НА ПРОФИЛИ, ПАРОЛИ И ДВУФАКТОРНА ЗАЩИТА

Чл. 11. Създаване на профили

(1) Профилите се създават служебно от Системния администратор или от друго изрично упълномощено лице.

(2) За ученическия профил се използва минимално необходимият обем информация, включително име, фамилия, училищен електронен адрес, клас и организационна единица.

(3) Единен граждански номер не се включва в потребителското име или електронния адрес.

(4) Потребителят няма право:

1. да предоставя профила си за ползване на друго лице;
2. да влиза в чужд профил;
3. да се представя за друг потребител;
4. да създава допълнителни или неразрешени училищни профили;
5. да прави опити за заобикаляне на административните ограничения.

Чл. 12. Пароли



(1) Първоначалната парола се създава или задава от Системния администратор.

(2) Данните за първоначален достъп се предоставят по защитен начин:

1. на ученика;
2. на родителя или настойника, когато възрастта на ученика и училищната организация налагат това;
3. чрез класния ръководител, когато той е определен единствено като лице за предаване на данните.

(3) Класният ръководител не поддържа постоянен, общодостъпен списък с действащите пароли на учениците.

(4) Паролата е лична и поверителна. Забранява се:

1. съобщаването ѝ на съученици или други лица;
2. изпращането ѝ чрез незащитени съобщения;
3. поставянето ѝ върху устройство или на видимо място;
4. използването на една и съща парола за училищния профил и лични профили;
5. съхраняването ѝ в публичен или споделен файл.

(5) При съмнение, че паролата е станала известна на друго лице, потребителят незабавно уведомява учител или Системния администратор.

(6) Системният администратор има право да изисква промяна на паролата, да я нулира или временно да блокира профила при риск за сигурността.

Чл. 13. Двухфакторно удостоверяване

(1) Двухфакторното удостоверяване е задължително за:

1. директора;
2. заместник-директорите;
3. Системните администратори;
4. учителите;
5. административните и останалите служители с училищни профили.



(2) Учениците влизат в профилите си с потребителско име и парола, без задължително използване на двуфакторно удостоверяване и без задължително въвеждане на динамични кодове.

(3) Системният администратор може да прилага допълнителни мерки за защита на ученическите профили, които не изискват предоставяне на личен телефонен номер от ученика.

IV. ИЗПОЛЗВАНЕ НА УСТРОЙСТВА

Чл. 14. Училищни и лични устройства

(1) Потребителите могат да използват училищните си профили от:

1. управлявани от Училището Chromebook устройства;
2. училищни компютри;
3. личен компютър;
4. таблет;
5. смартфон;
6. друго разрешено устройство.

(2) При използване на лично устройство потребителят носи отговорност за:

1. защитата на устройството с парола, код или биометрично заключване;
2. актуализирането на операционната система и приложенията;
3. използването на надеждна интернет връзка;
4. недопускането на достъп от неоторизирани лица;
5. излизането от училищния профил при предоставяне на устройството на друго лице.

(3) Влизането в училищен профил от обществен или чужд компютър се допуска само при необходимост.

(4) След приключване на работа на споделено или чуждо устройство потребителят е длъжен:



1. да излезе от профила чрез командата „Изход“/„Sign out“;
2. да затвори всички отворени прозорци;
3. да не запазва паролата в браузъра;
4. да премахне профила от устройството, когато е бил добавен към него;
5. да провери дали файлове не са останали изтеглени локално.

(5) При изгубено или откраднато устройство, на което има активен училищен профил, потребителят или родителят незабавно уведомява Системния администратор.

(6) Когато вреда е причинена или улеснена от неспазване на настоящите правила, отговорността се определя след изясняване на конкретните факти, вината, действията на Училището и приложимото законодателство. Училището не се освобождава предварително от законово установените си задължения за защита на информацията.

V. ДОПУСТИМА УПОТРЕБА, ОГРАНИЧЕНИЯ И ЗАБРАНИ

Чл. 15. Допустима употреба

(1) Училищният профил се използва за:

1. участие в учебни занятия;
2. достъп до Google Classroom;
3. получаване и изпълнение на задания;
4. създаване и споделяне на учебно съдържание;
5. комуникация с учители и съученици по учебни въпроси;
6. участие в училищни проекти;
7. работа по национални и международни образователни проекти;
8. изпълнение на служебни задължения;
9. други дейности, изрично одобрени от Училището.

(2) Използването трябва да бъде законосъобразно, добросъвестно, съобразено с възрастта на ученика и с принципите на дигиталната етика.

Чл. 16. Забрана за лични и неразрешени цели



Забранява се използването на училищния профил за:

1. създаване на лични профили във Facebook, Instagram, TikTok, Snapchat, Discord или други социални мрежи;
2. създаване на лични или публични YouTube канали без писмено разрешение;
3. регистрация в платформи за онлайн игри;
4. участие в хазартни дейности;
5. регистрация в онлайн магазини и търговски сайтове за лични покупки;
6. абонаменти за несвързани с обучението услуги;
7. масово изпращане на нежелани съобщения;
8. лична рекламна, търговска или политическа дейност;
9. организиране на частни събития, които не са свързани с Училището;
10. заобикаляне на филтри, ограничения и административни настройки;
11. използване на VPN, прокси, анонимизиращи услуги или други средства с цел преодоляване на училищните ограничения;
12. съхраняване или разпространяване на незаконно съдържание.

Изключение се допуска за предварително планирана учебна дейност, одобрена от учител и технически разрешена от Системния администратор.

Чл. 17. Дигитална етика и кибертормоз

(1) Забранява се използването на училищната среда за:

1. обиди, унижение и заплахи;
2. реч на омразата;
3. дискриминационно или нецензурно съдържание;
4. кибертормоз;
5. разпространяване на слухове;
6. злепоставяне на ученици, родители, учители или служители;
7. създаване и разпространяване на фалшиви профили;
8. изпращане на манипулирани снимки, аудио- или видеоматериали;
9. създаване или разпространяване на подвеждащо съдържание чрез изкуствен интелект;
10. публикуване на чужда кореспонденция без основание;



11. заснемане или записване на онлайн среща без предварително разрешение;
12. разкриване на лични данни на друго лице.

(2) Забранява се споделянето на снимки, видеозаписи, гласови записи, оценки, медицински данни, адреси, телефонни номера и друга лична информация за друго лице без подходящо основание и разрешение.

(3) Всеки потребител, който стане свидетел или получи информация за кибертормоз, е длъжен да уведоми учител, класен ръководител, член на ръководството или Системния администратор.

Чл. 18. Авторско право

(1) Потребителите са длъжни да спазват авторските и сродните права.

(2) При използване на чужди текстове, изображения, музика, видео, графики и други произведения се посочва източникът и авторът, когато това е приложимо.

(3) Забранява се:

1. представянето на чуждо съдържание като собствено;
2. копирането на готови разработки без посочване на източник;
3. незаконното разпространяване на учебници, книги, филми, музика или софтуер;
4. споделянето на закупени или лицензирани материали извън разрешения кръг;
5. използването на изкуствен интелект в нарушение на конкретно поставена учебна задача.

(4) Използването на изкуствен интелект се обозначава, когато това е изискано от учителя или от правилата за конкретната задача.

Чл. 19. Задължения на учителите и служителите

(1) Учителите и служителите не трябва да въвеждат в неразрешени външни платформи или публични AI инструменти:

1. имена и други идентификатори на ученици;



2. оценки и индивидуална обратна връзка;
3. медицински или психологически данни;
4. информация за специални образователни потребности;
5. данни за поведението или семейната среда;
6. служебни пароли и кодове;
7. непубликувани училищни документи;
8. договори, фактури и финансова информация;
9. поверителна кореспонденция;
10. други данни, защитени от закон или вътрешни правила.

(2) При работа в разрешени услуги учителят използва само необходимия минимум информация и проверява настройките за споделяне.

(3) Служебни документи не се съхраняват в лични Gmail, Drive или други лични облачни профили, освен ако това не е изрично разрешено поради техническа необходимост и са приложени подходящи мерки за защита.

VI. СПОДЕЛЯНЕ И КОМУНИКАЦИЯ

Чл. 20. Споделяне на файлове

(1) По правило файловете се споделят само с конкретни лица, класове или групи.

(2) Настройката „Всеки с връзката“ се използва само когато това е необходимо за конкретна образователна или публична училищна дейност.

(3) При файлове, съдържащи лични данни, оценки, индивидуална обратна връзка или служебна информация, публично споделяне не се допуска.

(4) Забранява се препращането на училищни файлове към лични профили или външни лица без разрешение.

(5) Учителят носи отговорност да зададе подходящи права:

1. „Преглед“;



2. „Коментар“;
3. „Редактиране“.

(6) Право на редактиране се предоставя само когато е необходимо за съвместната работа.

Чл. 21. Електронна комуникация

(1) Комуникацията чрез Gmail, Classroom, Chat и Meet трябва да бъде свързана с учебния процес или с дейността на Училището.

(2) Потребителите използват уважителен и професионален тон.

(3) Забранява се:

1. изпращането на съобщения до целия домейн без разрешение;
2. добавянето на външни лица в училищни групи и разговори без основание;
3. препращането на вътрешна кореспонденция;
4. изпращането на големи файлове или множество съобщения с цел претоварване на системата;
5. използването на скрити получатели за подвеждащи или неразрешени цели.

VII. МОНИТОРИНГ, КОНТРОЛ И ПРАВА НА АДМИНИСТРАТОРА

Чл. 22. Принципи на административния контрол

(1) Училището не извършва постоянно и безцелно наблюдение на личната учебна комуникация на потребителите.

(2) Административен контрол се извършва само когато е необходим за:

1. осигуряване на сигурността;
2. техническа поддръжка;
3. установяване на нарушение;
4. защита на ученик или друго лице;
5. разследване на кибертормоз;
6. възстановяване на изгубена или повредена служебна информация;



7. изпълнение на законово задължение;
8. изпълнение на валидно искане на компетентен орган.

(3) Контролът се извършва при спазване на принципите на необходимост, пропорционалност, ограничаване на целта и минимизиране на данните.

Чл. 23. Проверка при съмнение за нарушение

(1) Проверка може да бъде започната при:

1. писмен сигнал;
2. документирана устна жалба;
3. автоматично предупреждение за сигурност;
4. установена необичайна активност;
5. съмнение за компрометиран профил;
6. данни за кибертормоз;
7. съмнение за изтичане или неправомерно споделяне на информация.

(2) По правило първо се проверяват:

1. системните логове;
2. историята на влизанията;
3. настройките за споделяне;
4. свързаните приложения;
5. административните промени;
6. наличните предупреждения за сигурност.

(3) Достъп до съдържание на съобщения или файлове се извършва само когато:

1. това е необходимо за изясняване на случая;
2. целта не може да бъде постигната чрез по-малко intrusive средства;
3. има разрешение от директора или изрично упълномощено от него лице;
4. достъпът е ограничен до конкретните данни и период;
5. действията са документирани.



(4) При непосредствен риск за сигурността, живота, здравето или правата на дете Системният администратор може да предприеме спешни ограничителни действия, като незабавно докладва на директора.

(5) Информацията, установена при проверката, се предоставя само на лицата, които имат служебна необходимост да я получат.

Чл. 24. Временно ограничаване на профил

(1) Системният администратор има право временно да блокира или ограничи профил при:

1. компрометирана парола;
2. подозрение за неоторизиран достъп;
3. разпространение на вредоносен софтуер;
4. масово изпращане на нежелани съобщения;
5. опит за заобикаляне на административни ограничения;
6. непосредствен риск от загуба или изтичане на данни;
7. необходимост от запазване на доказателства.

(2) Блокирането не представлява дисциплинарна санкция, когато е предприето като временна техническа мярка за сигурност.

(3) За предприетата мярка се уведомяват директорът и засегнатият потребител, а когато потребителят е ученик – и неговият родител или настойник, освен ако временното отлагане на уведомяването е необходимо за защита на разследването или на друго лице.

VIII. ИНЦИДЕНТИ И ПРЕКРАТЯВАНЕ НА ДОСТЪПА

Чл. 25. Инциденти със сигурността

(1) Всеки потребител незабавно съобщава за:

1. изгубена или разкрита парола;
2. съмнително влизане;
3. получено фишинг съобщение;
4. изгубено или откраднато устройство;



5. изпратен по погрешка файл;
6. неправилно споделена папка;
7. изтрити или променени чужди материали;
8. вредоносен софтуер;
9. кибертормоз;
10. друга предполагаема злоупотреба.

(2) Потребителят не трябва самостоятелно да изтрива доказателства, съобщения или логове, свързани с инцидента.

(3) Системният администратор документира инцидента и предприетите действия.

(4) При нарушение на сигурността на личните данни директорът, длъжностното лице по защита на данните и Системният администратор преценяват необходимостта от уведомяване на Комисията за защита на личните данни и на засегнатите лица в предвидените от закона случаи и срокове.

Чл. 26. Прекратяване на профил

(1) Правото на използване на училищния профил се прекратява при:

1. преместване или завършване на ученика;
2. прекратяване на трудовото или гражданското правоотношение;
3. изтичане на срока на временния профил;
4. решение на директора в предвидените от закона случаи.

(2) При напускане профилът първо може да бъде временно блокиран, а след изтичане на определения срок – изтрит.

(3) Срокът за запазване, архивиране или изтриване на данните се определя съгласно:

1. законовите изисквания;
2. вътрешните правила за съхраняване на документи;
3. образователната и служебната необходимост;
4. лицензионните и техническите възможности.



(4) Преди прекратяване на ученически профил Училището може да предостави възможност на ученика да запази собствени учебни разработки, ако те:

1. не съдържат лични данни на други лица;
2. не са служебни или поверителни;
3. не нарушават авторски права;
4. не са предмет на проверка или спор.

(5) Училищна документация, класове в Classroom, служебни файлове и материали, необходими за продължаване на дейността, могат да бъдат прехвърлени на друг собственик или в споделено хранилище.

IX. ОТГОВОРНОСТ И САНКЦИИ

Чл. 27. Установяване на нарушение

(1) Преди налагане на мярка или санкция се изясняват:

1. конкретните действия;
2. авторът на нарушението;
3. наличието на вина;
4. причинените или възможните вреди;
5. възрастта и индивидуалните особености на ученика;
6. предходни нарушения;
7. предприетите от потребителя действия за ограничаване на вредите.

(2) Не се приема автоматично, че всяко действие, извършено от даден профил, е извършено лично от неговия титуляр. Проверят се данните за достъп и обстоятелствата по случая.

(3) На ученика се предоставя възможност да бъде изслушан и да даде обяснение.

(4) Родителят или настойникът се уведомява в предвидените от закона и вътрешните правила случаи.



Чл. 28. Мерки и санкции

(1) В зависимост от тежестта на нарушението могат да бъдат приложени:

1. устно или писмено предупреждение;
2. обучение или консултиране за безопасно използване;
3. задължителна промяна на паролата;
4. временно ограничаване на определена услуга;
5. временно блокиране на профила;
6. възстановителна или възпитателна мярка;
7. санкция по реда на Закона за предучилищното и училищното образование;
8. дисциплинарна отговорност за служител по реда на трудовото законодателство;
9. уведомяване на компетентен орган при данни за престъпление или друго тежко нарушение.

(2) Мерките трябва да бъдат съразмерни на нарушението и да отчитат най-добрия интерес на детето.

(3) Материална отговорност се търси само когато са установени вреда, противоправно поведение, причинна връзка и вина по приложимия законов ред.

Х. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 29.(1) Настоящите правила се приемат от компетентния орган на Училището и се утвърждават със заповед на директора.

(2) Правилата се довеждат до знанието на:

1. всички учители и служители – срещу подпис;
2. учениците – по подходящ за възрастта им начин;
3. родителите и настойниците – чрез декларация за запознаване.

(3) Родителското съгласие за Допълнителни услуги се събира отделно и конкретно, когато се изисква.



(4) Системният администратор извършва периодичен преглед на:

1. активираните услуги;
2. приложенията на трети страни;
3. външното споделяне;
4. административните права;
5. неактивните профили;
6. възрастовите настройки;
7. настройките за сигурност.

(5) Правилата се преразглеждат при:

1. промяна в законодателството;
2. промяна в условията или услугите на Google;
3. въвеждане на нова технология;
4. установен инцидент или нов риск;
5. промяна в организацията на училищната дейност.

(6) За неуредените въпроси се прилагат действащото законодателство, вътрешните правила на Училището и приложимите договорни условия за Google Workspace for Education



ПРИЛОЖЕНИЕ № 1

СЪГЛАСИЕ ЗА ИЗПОЛЗВАНЕ НА ДОПЪЛНИТЕЛНИ УСЛУГИ НА GOOGLE

Относно използването от детето ми

.....

чрез неговия/нейния училищен профил на Допълнителни услуги на Google, когато използването им е свързано с конкретна учебна дейност, урок, проект или друга образователна инициатива, организирана от Частно средно езиково училище „Д-р Мария Монтесори“ – гр. Бургас:

Информиран/а съм, че актуалният списък на Допълнителните услуги се поддържа от Google, като наличието на дадена услуга в този списък не означава, че тя автоматично е разрешена за учениците в училищния домейн.

Съгласието ми се отнася за Допълнителните услуги на Google, разрешени от Училището и посочени в чл. 4 от Вътрешните правила за работа с облачната платформа Google Workspace for Education.. То не включва използването на училищния профил за лични регистрации, лични канали, социални мрежи, онлайн покупки, игри или други дейности, които не са свързани с обучението.

Информиран/а съм, че мога да оттегля съгласието си с писмено заявление до директора на Училището.

☐ ДА, давам съгласието си.

☐ НЕ, не давам съгласието си.

Име на родителя/настойника:

Дата:.....

Подпис:



ПРИЛОЖЕНИЕ № 2

ДЕКЛАРАЦИЯ НА УЧЕНИКА

Аз, ...,

ученик/ученичка в клас в ЧСЕУ „Д-Р МАРИЯ МОНТЕСОРИ“ – ГР. БУРГАС,

декларирам, че съм запознат/а по разбираем за мен начин **с правилата за използване на училищния профил и се задължавам:**

1. да пазя паролата си;
2. да не влизам в чужд профил;
3. да използвам профила само за учебни цели;
4. да не обиждам, заплашвам или запустявам други лица;
5. да не споделям снимки, записи или лични данни на други хора без разрешение;
6. да не използвам училищния профил за социални мрежи, игри и покупки;
7. да съобщавам на учител или родител при съмнение за злоупотреба;
8. да излизам от профила си след работа на чуждо или споделено устройство;
9. да спазвам авторските права и правилата за използване на изкуствен интелект;
10. да изпълнявам указанията на учителите и Системния администратор.

Дата: Г.

Подпис на ученика:



ПРИЛОЖЕНИЕ № 3

СЪГЛАСИЕ ЗА СЪЗДАВАНЕ И ИЗПОЛЗВАНЕ НА УЧЕНИЧЕСКИ ПРОФИЛ В GOOGLE WORKSPACE FOR EDUCATION

Долуподписаният/ата:.....,

родител/настойник на:,

ученик/ученичка в клас в ЧСЕУ „Д-р Мария Монтесори“ – гр. Бургас,

ДАВАМ / НЕ ДАВАМ

(ненужното се зачертава)

съгласие Частно средно езиково училище „Д-р Мария Монтесори“ – гр. Бургас да създаде, администрира и поддържа училищен профил на детето ми в Google Workspace for Education за нуждите на образователния процес, учебната комуникация, създаването и предаването на учебни материали, съвместната работа и участието в организирани от Училището дейности и проекти.

Информиран/а съм, че при използването на училищния профил Google обработва информация, свързана с профила и използването на услугите, само за целите и при условията, описани във **„Вътрешни правила за работа с облачната платформа Google Workspace for Education“ на ЧСЕУ „Д-р Мария Монтесори“ – гр. Бургас**, публикувани на официалния интернет сайт на училището.

Декларирам, че съм запознат/а с посочените документи и с правилата за създаване, използване, защита, временно ограничаване и прекратяване на училищния профил.

Информиран/а съм, че училищният профил е предназначен единствено за учебни и служебно организирани дейности и не следва да се използва за лични регистрации, социални мрежи, онлайн игри, покупки или други цели, които не са свързани с дейността на Училището.

Дата:

Подпис:



МОНТЕСОРИ
ЧАСТНО СРЕДНО ЕЗИКОВО УЧИЛИЩЕ БУРГАС

гр. Бургас 8000, к-с Зорница, срещу бл. 13
тел.: +359 876 400 627, +359 879 400 194
www.montessorischool.bg | director@montessorischool.bg
