ОБЕДИНЕНО УЧИЛИЩЕ “ОТЕЦ ПАИСИЙ”

с. РАДОМИРЦИ, общ. ЧЕРВЕН БРЯГ, обл. ПЛЕВЕН, ул. “СКОБЕЛЕВ” № 3,
тел.: 06576 2269, 0879250143, ou radomirci@abv.bg

УТВЪРЖДАВАМ:х
ДИРЕКТОР: Атанаска Дичкова
Заповед № ...../..... г.

ВЪТРЕШНИ ПРАВИЛА

ЗА КИБЕРСИГУРНОСТ И ИНФОРМАЦИОННА СИГУРНОСТ В

ОБЕДИНЕНО УЧИЛИЩЕ „Отец Паисий“

ГЛАВА ПЪРВА

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите правила уреждат организацията, управлението, контрола и мерките за осигуряване на киберсигурността и информационната сигурност в училището.

Чл. 2. Основната цел на правилата е:

1. Да осигурят защита на информационните системи, компютърната техника и електронните ресурси на училището.
2. Да предотвратят неправомерен достъп до училищната информационна инфраструктура.
3. Да гарантират сигурността и поверителността на личните данни на учениците, родителите и служителите.
4. Да ограничат рисковете от вируси, зловреден софтуер, фишинг атаки и други киберзаплахи.
5. Да създадат условия за безопасно използване на интернет и дигиталните технологии в образователния процес.

Чл. 3. Правилата са задължителни за:

1. Директора.
2. Педагогическите специалисти.
3. Непедагогическия персонал.
4. Учениците – в частта, отнасяща се до използването на училищните информационни ресурси.

5. Външни лица и изпълнители, получили достъп до информационните системи на училището.

ГЛАВА ВТОРА

ОРГАНИЗАЦИЯ И ОТГОВОРНОСТИ

Чл. 4. Директорът на училището:

1. Организира и контролира изпълнението на настоящите правила.
2. Определя със заповед отговорно лице за координация на дейностите по информационна сигурност.
3. Осигурява условия за поддържане и защита на училищната информационна инфраструктура.
4. Организира запознаването на персонала с правилата.
5. Предприема действия при установени нарушения и инциденти.

Чл. 5. Определеното от директора отговорно лице:

1. Следи за правилното функциониране на компютърните системи и училищната мрежа.
2. Контролира актуализацията на операционните системи и използвания софтуер.
3. Следи за наличието и актуалността на антивирусната защита.
4. Подпомага служителите при възникнали проблеми с информационните технологии.
5. Съдейства при установяване и отстраняване на инциденти с информационната сигурност.
6. Организира или координира архивирането на важната училищна информация.

Чл. 6. Всеки служител е длъжен:

1. Да спазва настоящите правила.
2. Да използва предоставените му информационни ресурси само за служебни и образователни цели.
3. Да не предоставя своите пароли и потребителски профили на други лица.
4. Да не допуска неправомерен достъп до служебна информация.
5. Незабавно да уведомява директора или определеното отговорно лице при съмнение за пробив в сигурността.

ГЛАВА ТРЕТА

ПРАВИЛА ЗА ИЗПОЛЗВАНЕ НА КОМПЮТЪРНАТА ТЕХНИКА И ИНТЕРНЕТ

Чл. 7. Компютърната техника, периферните устройства и интернет връзката се използват за осъществяване на образователния процес и административната дейност на училището.

Чл. 8. На служителите се забранява:

1. Инсталирането на нелицензиран или неразрешен софтуер.
2. Изтеглянето и стартирането на файлове от съмнителни интернет източници.
3. Посещаването на сайтове с незаконно, вредно или неподходящо съдържание чрез училищната мрежа.
4. Използването на чужди потребителски профили.
5. Изключването или заобикалянето на антивирусната защита и други механизми за сигурност.
6. Свързването на неразрешени външни устройства към училищните компютри.

Чл. 9. При използване на интернет служителите трябва:

1. Да проверяват достоверността на интернет източниците.
2. Да не отварят съмнителни линкове и прикачени файлове.
3. Да не предоставят служебни данни в непроверени интернет платформи.
4. Да използват защитени връзки при достъп до служебни системи.
5. Да излизат от служебните си профили след приключване на работа, особено при използване на споделени компютри.

ГЛАВА ЧЕТВЪРТА

ЗАЩИТА НА ПОТРЕБИТЕЛСКИТЕ ПРОФИЛИ И ПАРОЛИТЕ

Чл. 10. Всеки служител използва индивидуален потребителски профил, когато системата позволява това.

Чл. 11. Паролите трябва:

1. Да бъдат достатъчно дълги и трудни за отгатване.
2. Да не съдържат лесно установими лични данни.
3. Да не се споделят с колеги, ученици или външни лица.
4. Да не се записват на видими и общодостъпни места.
5. Да бъдат променяни незабавно при съмнение за компрометиране.

Чл. 12. При наличие на техническа възможност се използва многофакторна автентикация за служебните електронни пощи и системи, съдържащи чувствителна информация.

Чл. 13. Достъпът до електронните дневници, образователните платформи и административните системи се предоставя съобразно служебните задължения на съответния служител.

ГЛАВА ПЕТА

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ И СЛУЖЕБНАТА ИНФОРМАЦИЯ

Чл. 14. Училището предприема организационни и технически мерки за защита на личните данни на:

1. Учениците.
2. Родителите и законните представители.

3. Педагогическите специалисти.
4. Непедагогическия персонал.
5. Други физически лица, чиито данни се обработват във връзка с дейността на училището.

Чл. 15. Служителите нямат право:

1. Да предоставят лични данни на ученици и родители на неоторизирани лица.
2. Да изпращат списъци с лични данни чрез незащитени канали.
3. Да публикуват лична информация в социални мрежи без съответното правно основание.
4. Да съхраняват служебни документи на лични устройства без разрешение и подходящи мерки за защита.
5. Да предоставят достъп до електронния дневник на други лица.
6. Да използват служебна информация за лични цели.

Чл. 16. Документите, съдържащи лични данни, се съхраняват на места и в информационни системи с ограничен достъп.

Чл. 17. Обработването и съхраняването на лични данни се извършва при спазване на приложимите изисквания на GDPR и Закона за защита на личните данни.

ГЛАВА ШЕСТА

КИБЕРСИГУРНОСТ В ОБРАЗОВАТЕЛНИЯ ПРОЦЕС

Чл. 18. Педагогическите специалисти носят отговорност за безопасното използване на дигиталните ресурси по време на учебните занятия.

Чл. 19. При използване на компютърни кабинети, интерактивни дисплеи, мултимедийни проектори и други електронни устройства учителите:

1. Следят за правилното използване на техниката.
2. Не допускат ученици да променят системните настройки без разрешение.
3. Контролират достъпа до интернет по време на учебните занятия.
4. Информират учениците за рисковете в онлайн средата.

Чл. 20. На учениците се забранява:

1. Да използват чужди потребителски профили.
2. Да правят опити за достъп до чужди файлове и системи.
3. Да инсталират софтуер без разрешение.
4. Да разпространяват вируси или други вредоносни програми.
5. Да осъществяват неоторизиран достъп до училищната мрежа.
6. Да заснемат и разпространяват лични данни и изображения на други лица в нарушение на приложимите правила.

Чл. 21. Учителите провеждат разяснителна работа с учениците относно:

1. Безопасно поведение в интернет.

2. Разпознаване на фалшиви профили и измамни съобщения.
3. Защита на личната информация.
4. Превенция на кибертормоза.
5. Отговорно използване на социалните мрежи.
6. Рисковете при използване на изкуствен интелект и непроверени дигитални приложения.

ГЛАВА СЕДМА

ЕЛЕКТРОННА ПОЩА И ДИГИТАЛНА КОМУНИКАЦИЯ

Чл. 22. Служебната електронна поща се използва за комуникация, свързана с дейността на училището.

Чл. 23. Забранява се:

1. Изпращането на служебна информация към непроверени адресати.
2. Отварянето на съмнителни прикачени файлове.
3. Изпращането на пароли и данни за достъп по електронна поща.
4. Използването на служебната електронна поща за нерегламентирани дейности.

Чл. 24. При получаване на съобщения с искане за пароли, банкови данни или друга поверителна информация служителите трябва да проверят автентичността на подателя.

ГЛАВА ОСМА

АРХИВИРАНЕ И ВЪЗСТАНОВЯВАНЕ НА ИНФОРМАЦИЯ

Чл. 25. Училището организира периодично архивиране на важната служебна информация, доколкото това е приложимо за използваните системи.

Чл. 26. Архивните копия се съхраняват при осигурена защита срещу неправомерен достъп, загуба и унищожаване.

Чл. 27. При загуба или повреждане на информация се предприемат действия за възстановяването ѝ от наличните архивни копия.

ГЛАВА ДЕВЕТА

РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ С КИБЕРСИГУРНОСТТА

Чл. 28. За инциденти с информационната сигурност се считат:

1. Заразяване на компютър с вирус или зловреден софтуер.
2. Неоторизиран достъп до електронна поща или информационна система.
3. Загуба или кражба на устройство, съдържащо служебна информация.
4. Изтичане или неправомерно разпространение на лични данни.
5. Фишинг атаки и измамни електронни съобщения.

6. Блокиране или нарушаване на работата на училищните информационни системи.

Чл. 29. При установяване на инцидент служителят:

1. Незабавно уведомява директора и определеното отговорно лице.
2. Преустановява работата със засегнатото устройство, когато това е необходимо за ограничаване на риска.
3. Не предприема самоволни действия по изтриване на файлове или промяна на системни настройки.
4. Предоставя информация за установения проблем.
5. Съдейства за ограничаване на последствията.

Чл. 30. Директорът организира:

1. Оценка на възникналия инцидент.
2. Предприемане на действия за ограничаване на последствията.
3. Уведомяване на компетентните органи, когато това се изисква.
4. Документиране на инцидента и предприетите мерки.
5. Анализ на причините и мерки за недопускане на повторни инциденти.

Чл. 31. При нарушение на сигурността на личните данни се прилагат съответните процедури за уведомяване съгласно GDPR, включително сроковете по чл. 33 и чл. 34, когато са приложими.

ГЛАВА ДЕСЕТА

ИЗПОЛЗВАНЕ НА ЛИЧНИ УСТРОЙСТВА И ОБЛАЧНИ УСЛУГИ

Чл. 32. Използването на лични компютри, телефони и таблети за достъп до служебна информация се допуска при спазване на определените от училището изисквания за сигурност.

Чл. 33. Не се допуска съхраняването на служебна информация в лични облачни профили без разрешение и оценка на сигурността.

Чл. 34. При използване на облачни платформи, образователни приложения и системи за електронно обучение се спазват изискванията за защита на личните данни.

ГЛАВА ЕДИНАДЕСЕТА

ОБУЧЕНИЕ И ПОВИШАВАНЕ НА ИНФОРМАЦИОННАТА КУЛТУРА

Чл. 35. Училището организира периодично информиране и обучение на служителите по въпроси, свързани с:

1. Киберсигурност.
2. Защита на личните данни.
3. Разпознаване на фишинг атаки.
4. Безопасно използване на интернет.

5. Превенция на кибертормоза.

Чл. 36. Учениците се запознават с основните правила за безопасност в интернет в рамките на учебния процес и часа на класа.

ГЛАВА ДВАНАДЕСЕТА

КОНТРОЛ И ОТГОВОРНОСТ

Чл. 37. Контролът по изпълнението на настоящите правила се осъществява от директора и определените от него длъжностни лица.

Чл. 38. Нарушенията на правилата се разглеждат съобразно действащото законодателство, Правилника за дейността на училището и приложимите вътрешни документи.

Чл. 39. Всеки служител носи отговорност за действията си при използването на училищните информационни ресурси съобразно своите служебни задължения и приложимите нормативни разпоредби.

ГЛАВА ТРИНАДЕСЕТА

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящите вътрешни правила са утвърдени със заповед на директора на училището.

§ 2. Правилата се довеждат до знанието на всички педагогически и непедагогически специалисти срещу подпис.

§ 3. Учениците се запознават с приложимите за тях правила чрез класните ръководители.

§ 4. При промяна на нормативната уредба или при установена необходимост правилата се актуализират.

§ 5. Настоящите правила влизат в сила от датата на утвърждаването им със заповед на директора.