МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОД КРАСНОДАР "ДЕТСКИЙ САД КОМБИНИРОВАННОГО ВИДА 13"

Подписан: МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОД КРАСНОДАР "ДЕТСКИЙ САД КОМБИНИРОВАННОГО ВИДА 13"
DN: C=RU, S=Краснодарский край, STREET="ул. Карасунская, 99", L=гор. Краснодар, T=заведующий, O="МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОД КРАСНОДАР ""ДЕТСКИЙ САД КОМБИНИРОВАННОГО ВИДА 13""", ОГРН=1022301617535, СНИЛС=00276272725, ИНН ЮЛ=2310067753, ИНН=230801660074, E=lisenkoes-kzk@yandex.ru, G=Валентина Климентьевна, SN=Агафонова, CN="МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОД КРАСНОДАР ""ДЕТСКИЙ САД КОМБИНИРОВАННОГО ВИДА 13"""
Основание: Я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: место вашего подписания
Дата: 2024-09-27 15:11:10
Foxit Reader Версия: 9.6.0

Приложение 1
Утверждаю:
Заведующий МБДОУ МО г.Краснодар
«Детский сад № 13»
_____В.К.Агафонова

ПОЛОЖЕНИЕ о сайте муниципального бюджетного дошкольного образовательного учреждения муниципального образования г.Краснодар «Детский сад комбинированного вида № 13»

1. Общие положения

1.1. Положение о сайте МБДОУ МО г.Краснодар «Детский сад № 13» (далее – Положение) определяет статус, задачи, требования, принципы построения и структуру информационных материалов, размещаемых на официальном web-сайте МБДОУ МО г.Краснодар «Детский сад № 13» (далее по тексту – Сайт, ДОО), а также регламентирует функционирование Сайта ДОО.

1.2. Функционирование Сайта МБДОУ МО г.Краснодар «Детский сад № 13» регламентируется ст. 28-29 Федерального закона «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ, приказом Федеральной службы по надзору в сфере образования и науки от 04.08.2023 № 1493 «Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления информации», постановлением Правительства Российской Федерации «Об утверждении правил размещения на официальном сайте образовательной организации в информационнотелекоммуникационной сети «Интернет» и обновления информации об образовательной организации от 20 октября 2021 № 1802, приказом департамента образования администрации муниципального образования город Краснодар от 30.08.2024 № 1650 «Об утверждении Положения о сайте образовательного учреждения муниципального образования город Краснодар», настоящим Положением, приказами и распоряжениями руководителя ДОО.

1.3. Информационные ресурсы Сайта формируются как отражение различных аспектов деятельности ДОО.

1.4. Сайт содержит материалы, не противоречащие законодательству Российской Федерации.

1.5. Информация, представленная на Сайте, является открытой и общедоступной, если иное не определено специальными документами.

1.6. Права на все информационные материалы, размещенные на Сайте, принадлежат ДОО, кроме случаев, оговоренных в соглашениях с авторами работ.

1.7. Концепция и структура Сайта обсуждается всеми участниками образовательного процесса на заседаниях органов самоуправления ДОО и утверждается приказом руководителя ДОО.

1.8. Пользователем Сайта ДОО может быть любое лицо, имеющее технические возможности выхода в сеть Интернет.

2. Цели, задачи Сайта

2.1. Цель Сайта - поддержка процесса информатизации в образовательном учреждении путем развития единого образовательного информационного пространства, представление образовательного учреждения в Интернетсообществе. Целью Сайта дошкольной образовательной организации является оперативное и объективное информирование общественности о деятельности ДОО, включение ДОО в единое образовательное информационное пространство.

2.2. Задачи Сайта дошкольной образовательной организации:

- обеспечение открытости деятельности ДОО;
- реализация принципов единства культурного и образовательного пространства, демократического государственно-общественного управления ДОО;
- реализация прав граждан на доступ к открытой информации при соблюдении норм профессиональной этики педагогической деятельности и норм информационной безопасности;
- оперативного и объективного информирования общественности о развитии и результатах уставной деятельности ДОО, поступлении и расходовании материальных и финансовых средств;
- формирование целостного позитивного имиджа ДОО;
- совершенствование информированности граждан о качестве образовательных услуг в дошкольном учреждении;
- создание условий для взаимодействия участников образовательного процесса, социальных партнеров ДОО;
- осуществление обмена педагогическим опытом;
- стимулирование творческой активности педагогов и обучающихся (воспитанников).

3. Информационная структура Сайта

3.1. Сайт состоит из разделов и подразделов в соответствии с требованиями к официальным Сайтам образовательных организаций (Федеральный закон «Об

образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ, ст.29, приказ Федеральной службы по надзору в сфере образования и науки от 04.08.2023 № 1493) и оформляется в виде списка разделов и подразделов с кратким описанием.

3.2. Информационный ресурс сайта ДОО формируется из общественнозначимой информации для всех участников образовательного процесса в со- ответствии с уставной деятельностью ДОО.

3.3. Информационный ресурс сайта ДОО является открытым и общедоступным. Информация на сайте ДОО излагается общеупотребительными словами, понятными широкой аудитории.

3.4. Информация, размещаемая на сайте ДОО, не должна:

- нарушать авторское право;
- содержать ненормативную лексику;
- унижать честь, достоинство и деловую репутацию физических и юридических лиц;
- содержать государственную, коммерческую или иную, специально охраняемую тайну;
- содержать информационные материалы, которые содержат призывы к насилию и насильственному изменению основ конституционного строя, разжигающие социальную, расовую, межнациональную и религиозную рознь, пропаганду наркомании, экстремистских религиозных и политических идей;
- содержать материалы, запрещенные к опубликованию законодательством Российской Федерации;
- противоречить профессиональной этике в педагогической деятельности.

3.5. Информационная структура сайта ДОО определяется в соответствии с задачами реализации государственной политики в сфере образования.

3.6. Информационная структура сайта ДОО формируется из двух видов информационных материалов: обязательных к размещению на сайте ДОО (инвариантный блок) и рекомендуемых к размещению (вариативный блок).

3.7. Информационные материалы инвариантного блока являются обязательными к размещению на официальном сайте ДОО в соответствии с пунктом 2 статьи 29 Федерального закона «Об образовании в Российской Федерации».

3.8. Информационные материалы вариативного блока могут быть расширены ДОО и должны отвечать требованиям пунктов 3.1, 3.2, 3.3 настоящего Положения.

3.9. На Сайте дошкольной образовательной организации размещается обязательная информация согласно приложению № 1 к настоящему Положению.

3.10. Требования к формату предоставления информации и навигации на официальном сайте образовательной организации, указанные в приложении № 2 к настоящему Положению, обязательны к выполнению.

3.11. Информационное наполнение сайта осуществляется в порядке, определяемом приказом руководителя ДОО.

3.12. Департамент образования администрации муниципального образования может вносить рекомендации по содержанию сайта ДОО.

4. Организация функционирования Сайта

4.1. Для обеспечения функционирования Сайта приказом руководителя:

- из числа сотрудников назначается Администратор Сайта;
- назначаются лица ответственные за функционирование Сайта;
- определяется перечень и объем обязательной предоставляемой ответственными лицами информации;
- определяется зона ответственности назначенных лиц.

4.2. Организацию всех видов работ, обеспечивающих работоспособность сайта, обеспечение целостности и доступности Сайта, реализации правил разграничения доступа возлагается на Администратора Сайта.

4.3. Администратор сайта имеет следующие полномочия:

- создавать, удалять и редактировать информационное наполнение Сайта;
- модерировать сообщения на форуме и в блогах Сайта;
- создавать, удалять, редактировать учетные записи пользователей сайта ДОО.

4.4. Администратор Сайта осуществляет консультирование сотрудников ДОО, заинтересованных в размещении информации на Сайте, по реализации технических решений и текущим проблемам, связанным с информационным наполнением соответствующего раздела (подраздела).

4.5. Информация, предназначенная для размещения на Сайте, утверждается руководителем ДОО.

4.6. Текущие изменения структуры Сайта осуществляет Администратор по согласованию с руководителем ДОО.

4.7. Администратор Сайта имеет право:

- вносить предложения администрации ДОО по информационному наполнению Сайта по соответствующим разделам (подразделам);
- запрашивать информацию, необходимую для размещения на Сайте у администрации ДОО.

5. Организация информационного наполнения и сопровождения Сайта

5.1. Дошкольная образовательная организация обеспечивает координацию работ по информационному наполнению и обновлению официального сайта.

5.2. ДОО самостоятельно обеспечивает:

- постоянную поддержку сайта в работоспособном состоянии;
- взаимодействие с внешними информационнотелекоммуникационными сетями, сетью Интернет;
- проведение организационно-технических мероприятий по защите информации на сайте ДОО от несанкционированного доступа, уничтожения, модификации и блокирования доступа к ней, а также иных неправомерных действий в отношении нее;
- возможность копирования информации на резервный носитель, обеспечивающий ее восстановление;
- защиту от копирования авторских материалов;
- размещение на Сайте информации в виде файлов с возможностью сохранения на технических средствах пользователей и допускающем после сохранения возможность поиска и копирования фрагментов текста, а также в графическом формате виде графических образов оригиналов;
- доступ к размещенной информации без использования программного обеспечения, установка которого на технические средства пользователя информации требует заключения лицензионного или иного соглашения с правообладателем программного обеспечения, предусматривающего взимание с пользователя информации платы;
- соблюдение авторских прав при использовании программного обеспечения, применяемого при создании и функционировании сайта. – соответствие Требованиям к структуре официального сайта ДОО в информационно-телекоммуникационной сети «Интернет» и формату её представления.

5.3. Содержание сайта ДОО формируется на основе информации, предоставляемой участниками образовательного процесса ДОО.

5.4. Подготовка и размещение информационных материалов инвариантного блока сайта ДОО регламентируется должностными обязанностями сотрудников ДОО.

5.5. Сайт ДОО размещается на серверах МКУ КМЦИКТ «Старт» по защищенному протоколу соединения с обязательным предоставлением информации об адресе департаменту образования администрации муниципального образования город Краснодар.

5.6. Форумы, гостевые книги, блоги, образовательные платформы могут являться возможностью Сайта или быть созданы на других хостингах при условии обязательной модерации.

6. Ответственность и контроль

6.1. Ответственность за содержание и достоверность размещаемой на Сайте информации несет руководитель ДОО.

6.2. Дисциплинарная и иная предусмотренная действующим законодательством РФ ответственность за качество, своевременность и достоверность информационных материалов возлагается на ответственных лиц. Лица, ответственные за функционирование официального сайта ДОО, несут ответственность:

- за отсутствие на официальном сайте ДОО информации обязательной к размещению; – за несоответствие требованиям, предъявляемым к размещению информации; – за нарушение сроков обновления информации;
- за размещение на официальном сайте ДОО информации, противоречащей пп. 3.4 Положения;
- за размещение на официальном сайте ДОО недостоверной информации.
- 6.3. Ответственность за некачественное текущее сопровождение Сайта несет Администратор. Некачественное текущее сопровождение может выражаться:
- в несвоевременном размещении предоставляемой информации;
- в отсутствии даты размещения документа;
- в совершении действий, повлекших причинение вреда информационному ресурсу;
- в невыполнении необходимых программно-технических мер по обеспечению целостности и доступности информационного ресурса, разграничения доступа и обеспечения информационной безопасности.

6.4. Контроль функционирования Сайта осуществляет Администратор сайта ДОО.

7. Финансирование, материально-техническое обеспечение

7.1. Руководитель дошкольной образовательной организации может устанавливать доплату за администрирование Сайта.

7.2. Руководитель дошкольной образовательной организации вправе поощрять работников за активное участие в наполнении, развитии и популяризации официального сайта ДОО.

7.3. Оплата работы ответственных лиц по обеспечению функционирования официального сайта ОО из числа участников образовательного процесса производится согласно Положению об оплате труда ДОО.

Приложение № 1
к Обязательной информации для размещения на сайте МБДОУ МО г.Краснодар «Детский сад № 13»

ИНФОРМАЦИОННАЯ ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ ДЛЯ РАЗМЕЩЕНИЯ НА ОФИЦИАЛЬНЫХ ИНТЕРНЕТ-РЕСУРСАХ

С каждым годом молодежи в интернете становиться больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;
2. Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничь физический доступ к компьютеру для посторонних лиц;
6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;

7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд "WECA", что обозначало словосочетание "WirelessFidelity", который переводится как "беспроводная точность".

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура "Wi-Fi". Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает "высокая точность". Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какието номера;
2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
3. При использовании Wi-Fi отключи функцию "Общий доступ к файлам и принтерам". Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе;
4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно "https://";
6. В мобильном телефоне отключи функцию "Подключение к Wi-Fi автоматически". Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги. Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах. В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в не анонимных идентификация пользователя является обязательной. Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли - это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;;
4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
2. Не указывай в личной почте личную информацию. Например, лучше выбрать "музыкальный_фанат@" или "рок2013" вместо "тема13";
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;
6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на "Выйти". Кибербуллинг или виртуальное издевательство Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
2. Управляй своей киберрепутацией;
3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
5. Соблюдай свою виртуальную честь смолоду;
6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами.

Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений. Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств. Основные советы для безопасности мобильного телефона: Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какието платные услуги; Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге? Необходимо обновлять операционную систему твоего смартфона; Используй антивирусные программы для мобильных телефонов; Не загружай приложения от неизвестного источника, ведь они могут содержать

вредоносное программное обеспечение; После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies; Периодически проверяй, какие платные услуги активированы на твоем номере; Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь; Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это. Online игры Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции. Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов. В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
3. Не указывай личную информацию в профайле игры;
4. Уважай других участников по игре;
5. Не устанавливай неофициальные патчи и моды;
6. Используй сложные и разные пароли;
7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься "любимым" делом. Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей. На английском языке phishing читается как фишинг (от fishing - рыбная ловля, password - пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
5. Установи надежный пароль (PIN) на мобильный телефон;
6. Отключи сохранение пароля в браузере;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. "Цифровая репутация" - это твой имидж, который формируется из информации о тебе в интернете. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети. Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу. Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только "для друзей";
3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право Современные школьники - активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность. Термин "интеллектуальная собственность" относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права - это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете. Использование "пиратского" программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.

О портале

Сетевичок.рф - твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. А также принять участие в конкурсах и стать самым цифровым гражданином!

Приложение № 2
к Обязательной информации для размещения на сайте МБДОУ МО г.Краснодар «Детский сад № 13»

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

Определение термина "информационная безопасность детей" содержится в Федеральном законе N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону "информационная безопасность детей" - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В силу Федерального закона N 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;
2. информация, распространение которой ограничено среди детей определенных возрастных категорий.
3. К информации, запрещенной для распространения среди детей, относится:
4. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;
5. способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
6. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
7. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
8. оправдывающая противоправное поведение;
9. содержащая нецензурную брань;
10. содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

1. информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
2. вызывающая у детей страх, ужас или панику, в т.ч. представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
3. представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
4. содержащая бранные слова и выражения, не относящиеся к нецензурной брани. С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

Общие правила для родителей

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.

2. Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.

3. Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)

4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).

5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями. Возраст от 7 до 8 лет В Интернете ребенок старается посетить те или иные сайты, а

возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т.е. Родительский контроль или то, что вы сможете увидеть во временных файлах. В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

Советы по безопасности в сети Интернет для детей 7 - 8 лет

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что Вы наблюдаете за ним не потому что Вам это хочется, а потому что Вы беспокоитесь о его безопасности и всегда готовы ему помочь.
3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
4. Используйте специальные детские поисковые машины.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
8. Приучите детей советоваться с Вами перед опубликованием какойлибо информации средствами электронной почты, чатов, регистрационных форм и профилей.
9. Научите детей не загружать файлы, программы или музыку без вашего согласия.
10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.
11. В "белый" список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
13. Не делайте "табу" из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты "для взрослых".
14. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что

они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях. Возраст детей от 9 до 12 лет В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности для детей от 9 до 12 лет

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
2. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.
3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.
4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете.
7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
8. Позволяйте детям заходить только на сайты из "белого" списка, который создайте вместе с ними.
9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
10. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
11. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.
12. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.
13. Расскажите детям о порнографии в Интернете.
14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

15. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз. Возраст детей от 13 до 17 лет В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок "для взрослых". Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете. Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в "свободное плавание" по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете. Важно по-прежнему строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми.

    Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете.

    Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей. Советы по безопасности в этом возрасте от 13 до 17 лет

    1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов ("черный список"), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

    2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.

    3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

    4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

    5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

    6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

    7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена

сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

9. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам, о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

11. Приучите себя знакомиться с сайтами, которые посещают подростки.

12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.

13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.

Приложение № 3
к Обязательной информации для размещения на сайте МБДОУ МО г.Краснодар «Детский сад № 13»

Рекомендации для размещения документов, подтверждающих результаты профессиональной деятельности педагогических работников, на официальном сайте образовательной организации

Данные рекомендации разработаны в целях проведения завершающего этапа перехода процедуры аттестации педагогических работников на электронный документооборот в соответствии с письмом Департамента государственной политики в сфере общего образования Министерства образования и науки Российской Федерации от 21.03.2017 № 08-554 «О принятии мер по устранению избыточной отчётности» и адресованы педагогическим работникам, специалистам, ответственным за организацию проведения аттестации в муниципальном образовании город Краснодар и образовательных организациях (далее - ОО), руководителям ОО. Для объективности проведения всестороннего анализа профессиональной деятельности аттестуемых педагогических работников необходимо в доступном и структурированном виде представление аттестационных документов, что может быть обеспечено посредством размещения их на официальном сайте ОО.

С этой целью рекомендуется соблюдать следующие требования:

1. Руководителю ОО рекомендуется обеспечить создание на главной странице (в основном навигационном меню) официального сайта ОО раздела «Аттестация педагогических работников» (далее - Раздел) для размещения документов, подтверждающих результаты профессиональной деятельности аттестуемых педагогических работников с соблюдением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», приказа Федеральной службы по надзору в сфере образования и науки от 04.08.2023 № 1493 «Об утверждении требований к структуре официального сайта образовательной организации в информационно - телекоммуникационной сети «Интернет» и формату представления на нём информации», постановление Правительства Российской Федерации от 20.10.2021 № 1802 «Об утверждении правил размещения на официальном сайте образовательной организации в информационнотелекоммуникационной сети «Интернет» и обновления информации об образовательной организации, а также о признании утратившими силу некоторых актов и отдельных положений некоторых актов правительства Российской Федерации».

2. Доступ к Разделу должен быть обеспечен без дополнительной регистрации.

3. Раздел должен состоять из следующих подразделов:

1) «Нормативные документы» (не публикуются на сайте ОО, переход осуществляется по ссылке на официальный сайт ГБУ КК «Центр сопровождения образования» (ГБУКК ЦСО) http://rcdpo.ru /rasporyaditelnye-inormativnyye-dokumenty/);

2) «Аттестация в целях подтверждения соответствия занимаемой должности» (наполнение информацией данного подраздела относится к компетенции ОО);

3) «Результаты профессиональной деятельности педагогических работников, аттестуемых в целях установления квалификационной категории (первой, высшей)» (далее - Подраздел).

4. Информация в Подразделе должна иметь следующую структуру:

1) список аттестуемых педагогических работников с указанием фамилии, имени, отчества, должности, преподаваемого предмета (при необходимости), что является ссылкой для перехода на персональную страницу аттестуемого педагогического работника;

2) на персональной странице размещаются документы, подтверждающие результаты профессиональной деятельности педагогического работника, структурированные в соответствии с разделами и критериями, представленными в Перечнях критериев и показателей для оценки профессиональной деятельности педагогических работников ОО города Краснодара, аттестуемых в целях установления квалификационной категории, утвержденных приказом министерства образования, науки и молодёжной политики Краснодарского края № 1597 от 17.04.2017 «Об утверждении измерительных материалов для оценки профессиональной деятельности педагогических работников образовательных организаций Краснодарского края при проведении аттестации в целях установления квалификационных категорий в период апробации электронного документооборота» (далее - Перечни).

Документы педагогического работника, аттестуемого по должности «воспитатель», должны состоять из трех разделов:

- «Результативность профессиональной деятельности по выявлению и развитию у воспитанников способностей к научной (интеллектуальной), творческой, физкультурно-спортивной деятельности»;

- «Личный вклад педагогического работника в повышение качества образования и транслирование опыта практических результатов своей профессиональной деятельности»;

- «Результативность деятельности педагогического работника в профессиональном сообществе». Каждому разделу соответствует электронная папка, каждая из которых содержит количество файлов, соответствующее

количеству критериев Перечней; файл может включать 1 и более отсканированных документов.

5. Документы, размещаемые в Подразделе, должны быть представлены в формате скан-копий; несколько скан-копий документов, подтверждающих результаты по одному критерию, необходимо объединить в один файл в формате PDF, разрешение фотографий не менее 150 dpi (точек на дюйм).

6. Размещение документов на персональной странице педагогического работника осуществляется одновременно по всем разделам.

7. Документы необходимо оформлять в соответствии с требованиями делопроизводства, без исправлений, шрифтом TimesNewRoman 14 размера. Текст должен читаться без затруднений в масштабе 1:1.

8. В особых случаях, если размещение документов в Подразделе невозможно по объективным техническим причинам, ответственному за организацию проведения аттестации в ОО необходимо обратиться за помощью к ответственному в муниципальном образовании.

Приложение № 2 к
Положению о сайте МБДОУ МО г.Краснодар «Детский сад № 13»

ТРЕБОВАНИЯ

к формату предоставления информации и навигации на официальном сайте МБДОУ МО г.Краснодар «Детский сад № 13»

Информация на официальном сайте дошкольной образовательной организации должна быть представлена в виде набора страниц и (или) иерархического списка, и (или) ссылок на другие разделы сайта. Информация должна иметь общий механизм навигации по всем страницам сайта. Механизм навигации должен быть представлен на каждой странице раздела. Доступ к разделу должен осуществляться с главной (основной) страницы Сайта, а также из основного навигационного меню Сайта.

Страницы раздела должны быть доступны в информационнотелекоммуникационной сети «Интернет» без дополнительной регистрации, содержать информацию, указанную в пунктах 7 – 20 Приказа Рособрнадзора от 04.08.2024 № 1493 «Об утверждении Требований к структуре официального сайта образовательной организации в информационнотелекоммуникационной сети «Интернет», а также доступные для посетителей Сайта ссылки на файлы, содержащие информацию о назначении данных файлов.

Допускается размещение на сайте иной информации, которая размещается, опубликовывается по решению образовательной организации и (или) размещение, опубликование которой является обязательным в соответствии с законодательством Российской Федерации.

1. Сайт должен иметь версию для слабовидящих (для инвалидов и лиц с ограниченными возможностями здоровья по зрению).
2. Информация на Сайте размещается в текстовом, гипертекстовом, графическом форматах, а также в форматах инфографики, мультимедиа, электронного документа, открытых данных и базы данных.
3. Информация в виде текста размещается на Сайте в формате, обеспечивающем возможность поиска и копирования фрагментов текста средствами браузера.

4. Текстовые и табличные материалы дополнительно к гипертекстовому формату размещаются на Сайте в виде файлов в формате, обеспечивающем возможность их сохранения на технических средствах пользователей (скачивание) и допускающем после сохранения возможность поиска и копирования произвольного фрагмента текста средствами соответствующей программы для просмотра.
5. Посредством применения форматов представления информации, размещенной на Сайте, пользователю должны быть обеспечены: Приложение № 2 к Положению о сайте МБДОУ МО г.Краснодар «Детский сад № 13» а) свободный доступ к информации на основе общедоступного программного обеспечения. Доступ к информации не может быть обусловлен требованием применения пользователями определенных веб-обозревателей или установки иных технических средств программного обеспечения, предоставляющих доступ к указанной информации; б) возможность навигации, поиска и использования текстовой информации при выключенной функции отображения графических элементов страниц в веб-обозревателе; в) возможность прочтения отсканированного текста в электронной копии документа, изготовленного на бумажном носителе.
6. Информация, указанная в пунктах 7 - 20 Приказа Рособрнадзора от 04.08.2024 № 1493 «Об утверждении Требований к структуре официального сайта образовательной организации в информационнотелекоммуникационной сети «Интернет», представляется на Сайте в формате, обеспечивающем ее автоматическую обработку, в целях повторного использования информации без предварительного изменения человеком.
7. Все страницы официального сайта, содержащие сведения, указанные в пунктах 7 - 20 Приказа Рособрнадзора от 04.08.2024 № 1493 «Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет», должны содержать html-разметку, определяющую наличие соответствующей информации, подлежащей размещению на Сайте. Данные, размеченные указанной html-разметкой, должны быть доступны для просмотра посетителями Сайта во всех подразделах раздела.