Муниципальное бюджетное общеобразовательное учреждение
Глубочанская средняя общеобразовательная школа № 8
347473 ул.Садовая, 27 х.Глубокий
Зимовниковский район, Ростовская область
тел: 34-1-43, 34-1-12. E-Mail: gsosh8@mail.ru

Приказ

от «18» августа 2021г. № 90

О назначении ответственных лиц
за безопасный доступ к сети «Интернет»
на 2021-2022 учебный год

В соответствии с Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», в целях реализации комплекса мер, направленных на ограничение доступа обучающихся МБОУ Глубочанской СОШ № 8 к видам информации, распространяемой посредством сети «Интернет»

приказываю:

1. Алпатову Л.Н., директора школы, назначить ответственным лицом за исполнение мониторинга по оснащению и использованию ИКТ ресурсов в образовательной деятельности МБОУ Глубочанской СОШ № 8 на 2021-2022 учебный год.
2. Кагальникову Галину Борисовну, учителя информатики, назначить ответственным лицом за ограничение (фильтрацию) доступа обучающихся к информации, не имеющей отношение к образовательной деятельности, при использовании ресурсов сети Интернет.
3. Магомедалиеву Зубайдат Магомедовну, заместителя директора, назначить ответственной за информатизацию образовательной деятельности в ОО, направленную на решение задач учебно-воспитательного характера.
4. Утвердить план мероприятий по обеспечению информационной безопасности в ОО на 2021-2022 учебный год (Приложение 1).
5. Утвердить форму журнала работы системы контентной фильтрации в ОО (Приложение 2).
6. Утвердить инструкцию для обучающихся по обеспечению информационной безопасности при использовании сети Интернет (Приложение 3).
7. Контроль исполнения данного приказа оставляю за собой.

Директор_____Л.Н.Алпатова

Ознакомлены:
Заместитель директора – Магомедалиева З.М. –
Учитель информатики – Кагальникова Г.Б. –

Приложение 1
к приказу от 18.08.2021г.№ 90

План мероприятий по обеспечению информационной безопасности
и безопасному использованию сети Интернет
В МБОУ Глубочанской СОШ № 8 на 2021-2022 учебный год

№ п/п	Направление деятельности и наименование мероприятия	Ответственные	Сроки
1. Создание организационно-правовых механизмов защиты детей от распространения информации, причиняющей вред их здоровью и развитию			
1.1.	Организация контроля за обеспечением защиты детей от распространения информации, причиняющей вред их здоровью и развитию, в соответствии с действующим законодательством.	Зам. директора, Учитель информатики	В течение учебного года
1.2.	Приведение локальных актов ОО, регламентирующих работу в сети Интернет, в соответствие с действующим законодательством.	Директор	Сентябрь 2021
1.3.	Проведение контроля функционирования интернет-ресурсов ОО	Учитель информатики	2 раза в месяц
1.4.	Организация профилактических мероприятий с родителями и обучающимися по вопросам информационной безопасности.	Зам. директора . Классные руководители	Октябрь 2021 - апрель 2022
1.5.	Осуществление педагогами контроля при работе обучающихся в сети Интернет.	Учителя, педагоги дополнительно-го образования	В течение учебного года
2. Информационное обеспечение и внедрение систем исключения доступа к информации, несовместимой с задачами образования и воспитания учащихся			
2.1.	Установка, настройка, проверка работоспособности и обеспечение бесперебойного функционирования программных средств контентной фильтрации, обеспечивающих исключение доступа обучающихся к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания обучающихся.	Учитель информатики	До 10.09.2021
2.2.	Обновление раздела «Информационная безопасность» официального сайта ОО по обеспечению информационной безопасности учащихся при использовании ресурсов сети Интернет.	Учитель информатики	Сентябрь 2021
2.3.	Мониторинг исключения доступа к Интернет-ресурсам, несовместимым с целями и задачами образования и воспитания обучающихся.	Учитель информатики	Ежеквартально
2.4.	Оформление уголка «Информационная безопасность».	Зам. директора, Учитель информатики	В течение учебного года
3. Профилактика у детей и подростков интернет-зависимости и правонарушений с использованием информационно- телекоммуникационных технологий, формирование у			

несовершеннолетних навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде			
3.1.	Включение в план работы ОО и организация мероприятий: - уроки, внеурочные занятия по теме «Информационная безопасность»; - обучающие мероприятия для педагогов по вопросам обеспечения организационных условий исключения доступа к Интернет-ресурсам, несовместимым с целями и задачами образования и воспитания; - родительские собрания по вопросам профилактики экстремистских проявлений среди учащихся, информационного противодействия терроризму в социальных сетях, блогах и на форумах	Зам. директора по ВР, учителя, классные руководители	Проведение - в течение года
3.2.	Участие в методических мероприятиях по созданию надежной системы защиты детей от противоправного контента в образовательной среде школы и дома, по вопросам ИКТ- компетентности учащихся.	Учителя, Классные руководители	В течение учебного года
4. Информационное просвещение граждан о возможности защиты детей от информации, причиняющей вред их здоровью и развитию			
4.1.	Включение в повестку совещаний педагогических работников ОО, родительских собраний вопросов обеспечения информационной безопасности детей при использовании ресурсов сети Интернет, профилактики у детей и подростков интернет-зависимости, игровой зависимости и правонарушений с использованием информационно- телекоммуникационных технологий, формирование у несовершеннолетних навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.	Заместители директора,	В течение учебного года
4.2.	Поддержание в актуальном состоянии на официальном сайте образовательной организации раздела «Информационная безопасность», публикация материалов по обеспечению информационной безопасности детей при использовании ресурсов сети Интернет.	Зам. директора	В течение учебного года
4.3.	Размещение на сайте школы ссылок на электронные адреса по проблемам информационной безопасности для всех участников образовательного процесса.	Учитель информатики	В течение учебного года
4.4.	Беседы с использованием материалов Интернет-ресурсов: «Интернет среди нас»; «Я и мои виртуальные друзья»; «Интернет в моей семье»; «Мой Интернет»; «Мой социум в Интернете»; «Интернет и моя будущая профессия»; «Интернет и моё здоровье».	Зам. директора, социальный педагог	В течение учебного года

Приложение 2
к приказу от 18.08.2021г.№ 90

Дата проверки	Ф.И.О. и должность проверяющего	Номер компьютера	Результаты проверки	Принятые меры	Подпись проверяющего

Приложение 3
к приказу от 18.08.2021г.№ 90

Инструкция для обучающихся по обеспечению информационной безопасности при использовании сети «Интернет» для размещения в учебных кабинетах, в которых осуществляется доступ в сеть «Интернет»

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 пачти (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. Ещ в 1991 году нидерландская компания зарегистрировала бренд "WECA", что обозначало словосочетание "Wireless Fidelity", 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 какие - то 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 неанонимных 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 сл 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 интернетсервисов.

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 какие - то 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, публич 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!

ИНСТРУКЦИЯ

ДЛЯ ОБУЧАЮЩИХСЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НЕЛЬЗЯ

1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей);
2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;
3. Грубить, придираться, оказывать давление - вести себя невежливо и агрессивно;
4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей;
5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь.

ОСТОРОЖНО

1. Не все пишут правду. Читаешь о себе неправду в Интернете - сообщи об этом своим родителям или опекунам;
2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха;
3. Незаконное копирование файлов в Интернете - воровство;
4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут;
5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

МОЖНО

1. Уважай других пользователей;
2. Пользуешься Интернет-источником - делай ссылку на него;
3. Открывай только те ссылки, в которых уверен;
4. Общаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут;
5. Пройди обучение на сайте "Сетевичок" и получи паспорт цифрового гражданина!

Муниципальное бюджетное общеобразовательное учреждение
Глубочанская средняя общеобразовательная школа № 8
347473 ул.Садовая, 27 х.Глубокий
Зимовниковскийрайон, Ростовская область
тел: 34-1-43, 34-1-12. E-Mail: gsosh8@mail.ru

Приказ

от «30» августа 2021 г. №113

О порядке использования на территории
МБОУ Глубочанской СОШ № 8
персональных устройств обучающихся,
имеющих возможность выхода в сеть «Интернет»

В соответствии с Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», письмом Министерства Российской Федерации от 07.06.2019 3 04-474 «О методических рекомендациях», Методическими рекомендациями об использовании устройств мобильной связи в общеобразовательных организациях» (утв. Роспотребнадзором № МР 2.4.0150-19, Рособрнадзором № 01-230/13-01 14.08.2019) в целях реализации комплекса мер, направленных на ограничение доступа обучающихся МБОУ Глубочанской СОШ № 8 к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования при использовании ими персональных устройств, имеющих возможность выхода в сеть «Интернет», на территории образовательного учреждения во время образовательного процесса

П Р И К А З Ы В А Ю:

1. Установить Порядок использования на территории МБОУ Глубочанской СОШ № 8 (далее ОО) персональных устройств обучающихся, имеющих возможность выхода в сеть «Интернет»:

1) Средства мобильной связи обучающихся могут использоваться в ОО для обмена информацией, определения местонахождения ребёнка, его самочувствия;
2) Пользование средствами мобильной связи обучающихся в здании ОО разрешается в перерывах между учебными занятиями, до и после завершения образовательного процесса;
3) В отдельных случаях использование средств мобильной связи обучающихся в образовательном процессе может быть допущено в целях реализации образовательных задач с разрешения учителя;
4) До урока, внеурочных мероприятий средства мобильной связи обучающихся должны быть отключены или переведены в режим «без звука»;
5) Средства мобильной связи обучающихся не должны находиться на партах, обеденных столах, иных поверхностях;
6) При использовании средств мобильной связи обучающихся в ОО обучающимся необходимо соблюдение норм:
   - не использовать в качестве звонка мелодии и звука, которые могут оскорбить

или встревожить окружающих;
- вести разговор с собеседником тихим голосом;
- категорически не использовать чужие средства мобильной связи, не сообщать номера средств мобильной связи третьим лицам без разрешения на то владельцев,
- при осуществлении фото-, видеосъёмки кого-либо при помощи средств мобильной связи, предварительно спрашивать на это разрешение.
7) обучающийся обязан знать:
- использование средств мобильной связи во время образовательного процесса является нарушением конституционного принципа: «осуществление прав и свобод гражданина не должно нарушать права и свободы других лиц» (п.3 ст.17 Конституции РФ),
- сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается (п.1 ст.24 Конституции РФ);
8) обучающимся запрещено:
- использовать средство мобильной связи в период образовательного процесса в любом режиме (в том числе как калькулятор, записную книжку, часы и т.д.),
- использовать средство мобильной связи как фото/видео камеру на уроках, прослушивать радио и музыку без наушников в помещении ОО;
- демонстрировать фотографии и снимки, оскорбляющие достоинство человека, пропагандировать жестокость и насилие, сознательно наносить вред имиджу ОО,
- подключить средство мобильной связи к электрическим сетям ОО для зарядки;
9) родителям (законным представителям) обучающихся не рекомендуется звонить своим детям (учащимся) во время образовательного процесса, следует ориентироваться на расписание звонков;
10) ответственность за сохранность средства мобильной связи обучающихся лежит на его владельце;
11) за оставленные в помещениях ОО средства мобильной связи образовательная организация ответственности не несёт, поиском пропажи не занимается.
2. Довести до сведения обучающихся Порядок использования на территории ОО персональных устройств обучающихся, имеющих возможность выхода в сеть «Интернет» под роспись в соответствии с Приложением 1.
Срок: до 05.09.2021
Отв.: классные руководители.
3.Довести до сведения родителей/законных представителей обучающихся Порядок использования на территории ОО персональных устройств обучающихся, имеющих возможность выхода в сеть «Интернет» под роспись в соответствии с Приложением 2.
Срок: до 05.09.2021
Отв.: классные руководители.
4. Оформить Согласие о снятии ответственности с руководителя ОО в случае предоставления родителями (законными представителями) обучающемуся персональных устройств обучающихся, имеющих возможность выхода в сеть «Интернет», при посещении ОО в соответствии с Приложением 3.
Срок: до 05.09.2021
Отв.: классные руководители.

5. Ознакомить обучающихся, родителей и педагогических работников с Памяткой для обучающихся, родителей и педагогических работников по профилактике неблагоприятных для здоровья и обучения детей эффектов от воздействия устройств мобильной связи.

Срок: до 05.09.2021

Отв.: Степаненко Г.Н., заместитель директора, классные руководители.

6. Контроль исполнения настоящего приказа оставляю за собой.

Директор Алпатова Л.Н.

С приказом ознакомлены:

Магомедалиева З.М.

Степаненко Г.Н.

Велья И.В.

Геращенко Е.А.

Крамарова Л.Ф.

Арифова Н.И.

Оруджева А.В.

Захаренко Е.И.

Сушко Л.И.

Багамаева П.Ш.

Клименко А.В.

Назаркина Т.П.

Богданова М.В.

Приложение №1
к приказу от 30.08.2021 №113

Ведомость
ознакомления обучающихся _____ класса МБОУ Глубочанской СОШ № 8 с Порядком использования на территории ОО персональных устройств обучающихся, имеющих возможность выхода в сеть «Интернет»

№	ФИ обучающегося	Подпись обучающегося	Подпись классного руководителя	Дата
1				
2				
3				

Приложение №2
к приказу от 30.08.2021 №113

Ведомость
ознакомления родителей (законных представителей) обучающихся _____ класса МБОУ Глубочанской СОШ № 8 с Порядком использования на территории ОО персональных устройств обучающихся, имеющих возможность выхода в сеть «Интернет»

№	ФИО родителя (законного представителя) обучающегося	Подпись родителя (законного представителя) обучающегося	Подпись классного руководителя	Дата
1				
2				
3				

Приложение №3
к приказу от 30.08.2021 №113

Согласие
о снятии ответственности с руководителя образовательной организации в случае предоставления родителями (законными представителями) обучающемуся персональных устройств, имеющих возможность выход в сеть «Интернет», при посещении образовательного учреждения

Я, _____
фамилия, имя, отчество родителей (законных представителей)
являясь родителем (законным представителем) _____
фамилия, имя ребёнка
ученика(цы) _____ класса МБОУ Глубочанской СОШ № 8 даю согласие о снятии ответственности с руководителя образовательной организации, реализующей мероприятия, направленные на защиту детей от видов информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в случае предоставления своему ребёнку персональных устройств, имеющих возможность выхода в сеть «Интернет», при посещении образовательного учреждения.

Дата _____ Подпись _____ Расшифровка _____

Приложение №4
к приказу от 30.08.2021 №113

Памятка
для обучающихся, родителей и педагогических работников по профилактике неблагоприятных для здоровья и обучения детей эффектов от воздействия устройств мобильной связи

1. Исключение ношения устройств мобильной связи на шее, поясе, в карманах одежды с целью снижения негативного влияния на здоровье.
2. Максимальное сокращение времени контакта с устройствами мобильной связи.
3. Максимальное удаление устройств мобильной связи от головы в момент соединения и разговора (с использованием громкой связи и гарнитуры).
4. Максимальное ограничение звонков с устройств мобильной связи в условиях неустойчивого приема сигнала сотовой связи (автобус, метро, поезд, автомобиль).
5. Размещение устройств мобильной связи на ночь на расстоянии более 2 метров от головы.

СОГЛАСОВАНО
на заседании педагогического совета
МБОУ Глубочанской СОШ № 8
Протокол от 27.08.2019г № 1

УТВЕРЖДАЮ
Директор
МБОУ Глубочанской СОШ № 8
_____ Л.Н.Алпатова
от 27.08.2019г. № 92

ПОЛОЖЕНИЕ
о правилах пользования устройствами мобильной связи и другими портативными электронными устройствами во время учебного процесса в МБОУ Глубочанской СОШ № 8

1. Общие положения

1.1. Настоящее положение использования средств мобильной связи (сотовые и спутниковые телефоны, смартфоны, планшеты и т. п.) и других портативных электронных устройств (электронные книги, MP3-плееры, ОУП плееры, диктофоны, электронные переводчики и т.п.) в здании и на территории МБОУ Глубочанской СОШ № 8 (далее – положение) устанавливается для обучающихся, их родителей (законных представителей), работников школы в целях улучшения работы школы, а также защиты гражданских прав всех участников образовательных отношений.

1.2. Положение разработано в соответствии с:

- Конституцией Российской Федерации,
- Федеральным законом от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации",
- Федеральным законом от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию",
- Федеральным законом от 27.07.2006 № 152 "О персональных данных",
- Методическими рекомендациями об использовании устройств мобильной связи в общеобразовательных учреждениях, утвержденных Федеральной службой по надзору в сфере образования и науки, приказ № 01-230/13-01 от 14.08.2019г.
- уставом и правилами внутреннего распорядка обучающихся школы.

1.3. Соблюдение положения:

- способствует праву каждого учащегося на получение образования в соответствии с федеральными государственными образовательными стандартами при реализации прав и свобод других лиц,
- способствует уменьшению вредного воздействия радиочастотного и электромагнитного излучения средств мобильной связи на участников образовательных отношений,
- обеспечивает защиту учащихся от пропаганды насилия, жестокости, порнографии и другой информации, причиняющей вред их здоровью и развитию,
- обеспечивает повышение уровня дисциплины,
- гарантирует психологически комфортные условия образовательного процесса.

2. Условия применения средств мобильной связи и других портативных электронных устройств в школе

2.1. Любой человек вправе пользоваться личными средствами мобильной связи, но не вправ ограничивать при этом других людей. Пользователи обязаны помнить о том, что использовани средств мобильной связи во время образовательного процесса является нарушение конституционного принципа о том, что «осуществление прав и свобод гражданина не должн нарушать права и свободы других лиц» (п.3 ст.17 Конституции РФ), следовательно, реализация и

права на получение информации (п.4 ст.29 Конституции РФ) является нарушением права других учащихся на получение образования (п.1 ст.43 Конституции РФ).

2.2. Пользователи обязаны помнить о том, что использование средств мобильной связи для сбора, хранения, использования и распространения информации о частной жизни лица без его согласия не допускается (п.1 ст.24 Конституции РФ).

2.3. Любой пользователь обязан знать и соблюдать следующие условия и правила пользования сотовыми телефонами и другими портативными электронными устройствами (смартфон, планшетный компьютер, электронные книги и др.) в школе:

- в здании школы **ставить телефон в беззвучный режим или оставлять в выключенном состоянии;**
- во время учебных, факультативных и иных занятиях мобильный телефон и другие портативные электронные устройства **необходимо в обязательном порядке убирать с рабочего стола;**
- недопустимо использование чужих средств мобильной связи и сообщение их номеров третьим лицам без разрешения на то владельцев.

2.4.В целях сохранности средств мобильной связи участники образовательного процесса обязаны:

- не оставлять свои средства мобильной связи без присмотра, в том числе в карманах верхней одежды;
- ни под каким предлогом не передавать мобильный телефон/электронные устройства в чужие руки (за исключением администрации школы);
- помнить, что ответственность за сохранность телефона и иных средств коммуникации лежит только на его владельце (родителях, законных представителях владельца).

2.5. Администрация, классные руководители и педагоги-предметники не несут материальной ответственности за утерянные средства мобильной связи и других портативных электронных устройств. За случайно оставленные в помещении образовательной организации сотовые телефоны/электронные устройства школа поиском пропажи не занимается. Все случаи хищения имущества рассматриваются по заявлению в полицию, в соответствии с действующим законодательством.

3. Пользователи имеют право:

3.1. Использование мобильной связи разрешается на переменах, а также до и после завершения образовательного процесса (т.е. ВНЕ уроков), в пределах допустимой нормы.

3.2. Необходимо соблюдать культуру пользования средствами мобильной связи:

- громко не разговаривать;
- не включать полифонию;
- при разговоре соблюдать правила общения.

4. Пользователям запрещается:

4.1.Использовать мобильный телефон и другие портативные электронные устройства НА УРОКЕ в любом режиме (в том числе как калькулятор, записную книжку, словарь иностранных слов, видеокамеру, видеоплеер, диктофон, игру и т.д.), за исключением занятий с применением ИК-технологий, подразумевающих использование планшетного компьютера или иных средств коммуникации.

4.2.Использовать громкий режим вызова и прослушивания мелодий во время пребывания в школе. Прослушивать радио и музыку без наушников.

4.3.Пропагандировать жестокость, насилие, порнографию и иные противоречащие закону действия посредством телефона и иных электронных устройств средств коммуникации.

4.4.Сознательно наносить вред имиджу школы.

4.5.Совершать фото и видеосъёмку в здании школы: без разрешения администрации в коммерческих целях; без согласия участников образовательного процесса в личных и иных целях.

5. Иные положения

5.1.Родителям (законным представителям) не рекомендуется звонить своим детям (учащимся) во

время образовательного процесса, следует ориентироваться на расписание звонков.
5.2.В случае форс-мажорных обстоятельств для связи со своими детьми во время образовательного процесса родителям (законным представителям) рекомендуется звонить классному руководителю или передавать сообщения по телефонам, размещённым на сайте школы и записанным в дневниках обучающихся.
5.3.При необходимости регулярного использования средств мобильной связи во время образовательного процесса пользователь должен предоставить директору школы аргументированное обоснование (медицинское заключение, объяснительную записку и т.д.) и получить письменное разрешение.
5.4.В случае форс-мажорных обстоятельств обучающиеся должны получить разрешение педагогического работника, осуществляющего образовательный процесс, на использование средств мобильной связи.

6. Ответственность за нарушение положения

За нарушение настоящего Положения предусматривается следующая ответственность:

6.1. За однократное нарушение учащемуся объявляется дисциплинарное взыскание в виде замечания (с написанием объяснительной).
6.2. При повторных фактах грубого нарушения (п.4.1. – 4.5.) – комиссионное изъятие средств мобильной связи и других портативных электронных устройств (планшеты, электронные книги, MP3-плееры, ОУП плееры, диктофоны, электронные переводчики и т.п.), предварительно получив на это согласие родителей (законных представителей), собеседование администрации школы с родителями (законными представителями) учащегося и передача им сотового телефона/электронного устройства, вплоть до запрета ношения в школу средств мобильной связи и других портативных электронных устройств на ограниченный срок.

6.3. За нарушение настоящего Положения, пользователи средств мобильной связи несут ответственность в соответствии с действующим законодательством и локальными актами школы.

7. Изменение положения

7.1. Настоящее положение имеет неограниченный срок действия.
7.2. Настоящее положение является локальным правовым актом школы и может быть изменено по решению Педагогического Совета школы. При изменении законодательства в акт вносятся изменения в установленном законом порядке

Приложение №1

Памятка для обучающихся, родителей и педагогических работников по профилактике неблагоприятных для здоровья и обучения детей эффектов от воздействия устройств мобильной связи

1. Исключение ношения устройств мобильной связи на шее, поясе, в карманах одежды с целью снижения негативного влияния на здоровье.
2. Максимальное сокращение времени контакта с устройствами мобильной связи.
3. Максимальное удаление устройств мобильной связи от головы в момент соединения и разговора (с использованием громкой связи и гарнитуры).
4. Максимальное ограничение звонков с устройств мобильной связи в условиях неустойчивого приема сигнала сотовой связи (автобус, метро, поезд, автомобиль).
5. Размещение устройств мобильной связи на ночь на расстоянии более 2 метров от головы.