УТВЕРЖДЕНО
приказом директора МАОУ гимназии
имени А.П.Чехова от 29.08.2026 №265

ПОЛОЖЕНИЕ
о внедрении Методических рекомендаций по регулированию вопросов, связанных с использованием цифровых технологий несовершеннолетними в зависимости от их возраста, объема использования, рисков и мероприятий по их снижению МАОУ гимназии имени А.П.Чехова

1. Общие положения

1.1. Настоящее Положение устанавливает в МАОУ гимназии имени А.П.Чехова (далее - Гимназия) организационные основы внедрения Методических рекомендаций по регулированию вопросов, связанных с использованием цифровых технологий несовершеннолетними в зависимости от их возраста, включая рекомендации по возрасту начала использования цифровых технологий, объему их использования, рискам и возможным мероприятиям по их снижению с учетом возрастной периодизации.
1.2. Положение направлено на формирование в Гимназии безопасной, здоровьесберегающей и развивающей цифровой образовательной среды, предупреждение негативного воздействия цифровых технологий на физическое, психическое, нравственное и социальное развитие несовершеннолетних, а также формирование у обучающихся навыков безопасного и ответственного поведения в цифровой среде.
1.3. Настоящее Положение разработано в соответствии с:
- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральным законом от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- санитарными правилами СП 2026 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи»;
- санитарными правилами и нормами СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания»;
- письмом Минобрнауки России от 24.07.2025 № МН-6/2164 «О направлении методических рекомендаций»;
- письмом Минпросвещения России от 04.06.2026 № 07-8526 «О направлении материалов»;
- Уставом Школы;
- Правилами внутреннего распорядка обучающихся (от 01.09.2026 г.);
1.4. Методические рекомендации, положенные в основу настоящего Положения, применяются с учетом действующих обязательных требований законодательства Российской Федерации, санитарных правил, законодательства о защите детей от информации, причиняющей вред их здоровью и развитию, законодательства о персональных данных и законодательства об образовании.
1.5. Настоящее Положение распространяется на:
- обучающихся Гимназии;
- педагогических работников;
- иных работников Гимназии, участвующих в организации образовательного и воспитательного

процесса;
- родителей (законных представителей) несовершеннолетних обучающихся в части взаимодействия со Гимназией и рекомендаций по формированию безопасных цифровых привычек детей.

1.6. Положение применяется при:
- организации учебных занятий с использованием электронных средств обучения;
- реализации внеурочной деятельности;
- организации воспитательной работы;
- реализации дополнительного образования;
- использовании цифровых образовательных ресурсов и сервисов;
- профилактической и просветительской работе с обучающимися и их родителями;
- организации самостоятельной работы обучающихся, если такая работа предполагает использование цифровых технологий;
- профилактике цифровой зависимости, кибербуллинга, вовлечения несовершеннолетних в деструктивные интернет-сообщества и иных рисков цифровой среды.

2. Основные понятия

2.1. Для целей настоящего Положения используются следующие основные понятия: **цифровые технологии** - совокупность программных, технических, информационных и телекоммуникационных средств, используемых для создания, обработки, хранения, передачи и получения цифровой информации;
цифровая среда - совокупность информационных ресурсов, информационных систем, интернет-сервисов, платформ, социальных сетей, мессенджеров, приложений, компьютерных программ и цифровых устройств, используемых несовершеннолетними;
электронные средства обучения (ЭСО) - технические средства, используемые в образовательном процессе для представления и обработки информации в электронной форме;
экранное время - период взаимодействия несовершеннолетнего с устройством, предполагающим визуальное восприятие информации с электронного экрана;
цифровая безопасность - состояние защищенности несовершеннолетнего от информационных, психологических, социальных, финансовых, технических и иных рисков цифровой среды;
цифровая гигиена - совокупность правил и навыков безопасного, разумного и здоровьесберегающего использования цифровых устройств и интернет-ресурсов;
вредоносный и деструктивный контент - информация, способная причинить вред здоровью, психическому, физическому, нравственному или социальному развитию ребенка либо запрещенная или ограниченная для распространения среди детей законодательством Российской Федерации.

3. Цели и задачи внедрения Методических рекомендаций

3.1. Целями внедрения Методических рекомендаций являются:
- обеспечение безопасного и педагогически обоснованного использования цифровых технологий несовершеннолетними;
- минимизация рисков, связанных с чрезмерным использованием цифровых устройств;
- сохранение физического и психического здоровья обучающихся;
- формирование цифровой культуры и цифровой грамотности;
- развитие критического мышления и способности оценивать достоверность цифрового контента;
- защита несовершеннолетних от вредной и противоправной информации;
- профилактика зависимого поведения, кибербуллинга, мошенничества, вовлечения в противоправные и деструктивные сообщества;
- обеспечение взаимодействия педагогов и родителей в вопросах безопасного использования детьми цифровых технологий.

3.2. Основными задачами являются:
3.2.1. Организация использования цифровых технологий с учетом возраста обучающихся.
3.2.2. Соблюдение санитарно-гигиенических требований к использованию электронных средств

обучения.
3.2.3. Формирование у обучающихся навыков самоконтроля при использовании цифровых устройств.
3.2.4. Информирование обучающихся о рисках цифровой среды.
3.2.5. Повышение компетентности педагогических работников и родителей в вопросах цифровой безопасности.
3.2.6. Организация профилактики негативных последствий чрезмерного экранного времени.
3.2.7. Формирование безопасного поведения при использовании социальных сетей, мессенджеров, онлайн-игр и иных цифровых сервисов.
3.2.8. Обеспечение защиты персональных данных обучающихся.
3.2.9. Формирование алгоритмов реагирования на случаи кибербуллинга, интернет-мошенничества, распространения запрещенного контента и иных цифровых рисков.

4. Основные принципы использования цифровых технологий несовершеннолетними

4.1. В Школе использование цифровых технологий строится на следующих принципах:
- законности;
- приоритета жизни и здоровья ребенка;
- соответствия цифрового контента возрасту обучающегося;
- педагогической целесообразности;
- дозированности экранной нагрузки;
- чередования цифровой и нецифровой деятельности;
- обеспечения двигательной активности;
- защиты персональных данных;
- профилактики информационных и психологических рисков;
- взаимодействия семьи и Гимназии;
- формирования самостоятельного ответственного поведения несовершеннолетнего в цифровой среде.

4.2. Использование цифровых средств не должно без объективной необходимости заменять непо деятельность, чтение печатных материалов, двигательную активность, творчество и иные формы деятельности, необходимые для полноценного развития ребенка.
4.3. При выборе цифровых ресурсов педагогический работник учитывает возраст обучающихся, содержание ресурса, его образовательную ценность, безопасность, отсутствие запрещенной информации, объем визуальной и информационной нагрузки.

5. Возрастной подход к использованию цифровых технологий

5.1. При организации профилактической, просветительской и воспитательной работы Гимназия учитывает возрастную периодизацию, предусмотренную Методическими рекомендациями.
5.2. Для детей младшего школьного возраста особое внимание уделяется:
- формированию навыков безопасного поиска информации;
- защите от случайного доступа к вредоносному контенту;
- формированию критического отношения к рекламе;
- предупреждению участия в опасных интернет-челленджах;
- недопущению передачи персональных данных незнакомым лицам;
- предупреждению интернет-мошенничества;
- ограничению бесконтрольного использования онлайн-игр и социальных сервисов.

5.3. Для обучающихся подросткового возраста особое внимание уделяется:
- профилактике вовлечения в деструктивные интернет-сообщества;
- противодействию кибербуллингу;
- профилактике интернет-зависимого поведения;
- формированию критического мышления;
- профилактике распространения персональных данных и интимного контента;
- предупреждению противоправных действий в сети Интернет;

- формированию навыков распознавания манипулятивного и экстремистского контента;
-профилактике вовлечения несовершеннолетних в финансовое мошенничество, незаконный оборот денежных средств и иные противоправные схемы.

5.4. Для старших подростков наряду с указанными направлениями обеспечивается развитие навыков осознанного цифрового поведения, самостоятельной оценки источников информации, защиты цифровой репутации и персональных данных.

5.5. Методическими рекомендациями предлагается ориентироваться на ограничение общего экранного времени с учетом возраста, в частности: для детей 7–11 лет — до 1,5 часа в день, для детей 11–16 лет — до 2 часов в день. Данные показатели используются Школой прежде всего в просветительской работе с родителями и обучающимися и не заменяют обязательные санитарные нормы, регулирующие использование электронных средств обучения в образовательной организации.

5.6. Родителям рекомендуется при организации досуга ребенка обеспечивать разумное чередование использования цифровых устройств с двигательной активностью, прогулками, чтением, творческой деятельностью, непосредственным семейным и социальным общением.

6. Использование электронных средств обучения в образовательном процессе

6.1. Использование ЭСО организуется с обязательным соблюдением действующих санитарно-эпидемиологических требований.

6.2. Педагогический работник при планировании урока определяет целесообразность применения ЭСО и продолжительность работы с ними.

6.3. Продолжительность непрерывного и суммарного использования ЭСО не должна превышать нормативов, установленных СанПиН 1.2.3685-21.

6.4. При использовании нескольких электронных средств обучения суммарная продолжительность работы определяется с учетом требований действующих санитарных норм.

6.5. Педагогические работники обеспечивают смену видов деятельности обучающихся.

6.6. При продолжительной зрительной нагрузке рекомендуется проведение упражнений для профилактики зрительного утомления, физкультурных минуток и иной двигательной активности.

6.7. При выборе форм домашней самостоятельной работы педагогам рекомендуется учитывать суммарную цифровую нагрузку обучающегося в течение дня.

6.8. Не допускается необоснованное увеличение количества заданий, выполнение которых требует длительного нахождения обучающегося перед экраном.

6.9. Если образовательный результат может быть достигнут равноценным способом без использования цифрового устройства, педагог вправе выбирать нецифровую форму работы.

7. Использование средств мобильной связи обучающимися

7.1. Обучающиеся не используют средства подвижной радиотелефонной связи во время учебных занятий при освоении образовательных программ начального общего, основного общего и среднего общего образования, за исключением случаев возникновения угрозы жизни или здоровью обучающихся, работников Гимназии, иных экстренных случаев.

7.2. Перед началом учебного занятия мобильное устройство переводится в беззвучный режим и убирается обучающимся в личные вещи, либо размещается в специально отведенное место (подставку) в классе, где проходит урок/занятие.

7.3. Порядок хранения мобильных устройств не должен создавать условий для необоснованного изъятия имущества обучающихся или возложения на работников Гимназии материальной ответственности за принадлежащие обучающимся устройства.

7.4. Использование мобильного телефона в экстренной ситуации допускается независимо от установленного общего ограничения.

7.5. Порядок использования мобильных средств связи на занятиях внеурочной деятельности, дополнительного образования на территории Гимназии тот же, что и на уроках.

8. Требования к цифровому контенту

8.1. При использовании цифровых ресурсов в образовательном процессе педагогические работники обязаны предварительно оценивать их содержание.
8.2. Не допускается целенаправленное предоставление обучающимся доступа к информации, распространение которой среди детей запрещено законодательством Российской Федерации.
8.3. При подборе образовательного контента учитываются возраст обучающихся и установленная информационной продукции возрастная категория.
8.4. Особое внимание уделяется предупреждению доступа обучающихся к информации:
- побуждающей к совершению действий, представляющих угрозу жизни и здоровью;
- содержащей способы совершения самоубийства или призывы к нему;
- пропагандирующей употребление наркотических, психотропных, одурманивающих веществ, алкоголя, табачной и никотинсодержащей продукции;
- вовлекающей несовершеннолетних в азартные игры;
- содержащей признаки экстремистской или террористической деятельности;
- побуждающей несовершеннолетних к противоправному поведению;
- содержащей иные виды информации, запрещенные или ограниченные законодательством для распространения среди детей.

8.5. На технических средствах Гимназии применяются предусмотренные законодательством и техническими возможностями средства контентной фильтрации и ограничения доступа к запрещенным ресурсам.

9. Профилактика основных рисков цифровой среды

9.1. Профилактическая работа в Гимназии организуется по следующим направлениям:

- чрезмерное экранное время;
- игровое и интернет-зависимое поведение;
- кибербуллинг;
- цифровое мошенничество;
- фишинг;
- незаконное получение и использование персональных данных;
- вовлечение несовершеннолетних в противоправные действия;
- распространение персональных данных и фотографий без согласия;
- деструктивные интернет-сообщества;
- опасные интернет-челленджи;
- распространение заведомо ложной информации;
- манипулятивное информационное воздействие;
- деструктивный, экстремистский и террористический контент;
- вредоносное программное обеспечение;
- риски онлайн-игр;
- финансовые риски и несанкционированные покупки;
- нарушение режима сна и двигательной активности вследствие использования цифровых устройств.

10. Формирование цифровой грамотности обучающихся

10.1. Гимназия обеспечивает систематическое формирование цифровой грамотности обучающихся в урочной, внеурочной и воспитательной деятельности.
10.2. Обучающиеся знакомятся с правилами:
- создания надежных паролей;
- защиты учетных записей;
- использования двухфакторной аутентификации при наличии такой возможности;
- безопасного общения с незнакомыми лицами в сети Интернет;
- распознавания мошеннических сообщений и сайтов;
- безопасной оплаты товаров и услуг;
- защиты банковских и иных конфиденциальных данных;

- проверки достоверности информации;
- соблюдения авторских прав;
- соблюдения правил сетевого этикета;
- защиты собственной цифровой репутации.
10.3. Обучающимся разъясняется недопустимость:
- передачи паролей третьим лицам;
- передачи незнакомым лицам банковских данных, кодов подтверждения и иных конфиденциальных сведений;
- размещения в открытом доступе избыточных персональных данных;
- распространения фотографий и персональной информации других лиц без законных оснований;
- участия в травле и унижении других пользователей;
- создания и распространения противоправного контента.

11. Профилактика кибербуллинга

11.1. Гимназия рассматривает кибербуллинг как одну из форм травли, реализуемую с использованием цифровых технологий.
11.2. Обучающийся, столкнувшийся с кибербуллингом, вправе обратиться к классному руководителю, педагогу-психологу, заместителю директора, директору.
11.3. При выявлении признаков кибербуллинга работник Гимназии:
- обеспечивает первичную безопасность ребенка;
- информирует администрацию в пределах установленного порядка;
- организует фиксацию имеющихся сведений о ситуации без дальнейшего распространения вредоносного контента;
- при необходимости привлекает педагога-психолога;
- информирует родителей (законных представителей), если иное не требуется исходя из необходимости защиты прав ребенка;
- организует меры по прекращению травли;
- при наличии признаков административного правонарушения, преступления или угрозы жизни и здоровью действует в соответствии с законодательством и локальными алгоритмами межведомственного взаимодействия.
11.4. Не допускается публичное обсуждение ситуации с раскрытием персональных данных пострадавшего несовершеннолетнего.

12. Защита персональных данных и цифровой репутации

12.1. Обработка персональных данных обучающихся осуществляется в соответствии с законодательством Российской Федерации.
12.2. Размещение фотографий, видеозаписей и иных материалов, содержащих персональные данные обучающихся, осуществляется при наличии предусмотренных законодательством оснований.
12.3. Педагогические работники не вправе требовать от обучающегося передачи пароля от личной учетной записи, личной электронной почты, социальных сетей или мессенджеров, если такая обязанность прямо не предусмотрена законодательством.
12.4. Не допускается создание работниками Гимназии условий, при которых обучающийся для получения обязательного образования вынужден использовать личный аккаунт в информационной системе, не предусмотренной организацией образовательного процесса и законодательством.
12.5. При использовании цифровых образовательных платформ Гимназия принимает меры по минимизации объема обрабатываемых персональных данных несовершеннолетних.

13. Обязанности педагогических работников

13.1. Педагогические работники:
- соблюдают санитарные требования при использовании ЭСО;

- предварительно оценивают используемый цифровой контент;
- учитывают возраст обучающихся;
- формируют навыки безопасного цифрового поведения;
- не допускают необоснованной цифровой перегрузки;
- своевременно реагируют на выявленные цифровые риски;
- участвуют в мероприятиях по повышению цифровой и медиаграмотности;
- информируют администрацию о выявлении контента или обстоятельств, создающих угрозу жизни, здоровью или безопасности обучающихся;
- соблюдают требования законодательства о персональных данных.
-

14. Функции классного руководителя

14.1. Классный руководитель:
- проводит классные часы и профилактические мероприятия по цифровой безопасности;
- информирует родителей о цифровых рисках;
- способствует формированию единых подходов семьи и Гимназии к использованию цифровых устройств;
- выявляет признаки неблагополучия, связанные с цифровой средой;
- при необходимости взаимодействует с педагогом-психологом, социальным педагогом и администрацией;
- доводит до обучающихся алгоритмы обращения за помощью;
- организует профилактику кибербуллинга и интернет-мошенничества.

15. Функции педагога-психолога

15.1. Педагог-психолог в пределах своей компетенции:
- участвует в профилактике зависимого и деструктивного цифрового поведения;
- проводит просветительскую работу;
- консультирует обучающихся и родителей;
- участвует в сопровождении детей, столкнувшихся с кибербуллингом, деструктивным контентом и иными цифровыми рисками;
- содействует формированию навыков эмоциональной саморегуляции;
- участвует в разработке индивидуальных профилактических мер при наличии оснований.

16. Функции заместителя директора по правовому воспитанию и профилактике правонарушений

16.1. Заместитель директора по ПВ:
- участвует в выявлении социальных рисков цифровой среды;
- организует профилактическую работу с обучающимися группы риска;
- участвует в межведомственном взаимодействии;
- проводит разъяснительную работу с семьями;
- участвует в реагировании на случаи вовлечения несовершеннолетних в противоправную деятельность посредством сети Интернет.

17. Обязанности обучающихся

17.1. Обучающиеся обязаны:
- соблюдать Правила внутреннего распорядка и настоящее Положение;
- выполнять требования законодательства об ограничении использования средств подвижной радиотелефонной связи во время учебных занятий;
- соблюдать правила информационной безопасности;
- уважать права, честь и достоинство других участников образовательных отношений;
- не использовать цифровые технологии для травли, угроз, распространения оскорблений или заведомо ложных сведений;

- не распространять запрещенную информацию;
- соблюдать правила защиты персональных данных;
- выполнять законные требования педагогических работников в части организации образовательного процесса.

17.2. Обучающийся вправе обратиться за помощью к любому педагогическому работнику при обнаружении угроз, травли, шантажа, мошенничества, противоправного контента или иных опасностей в цифровой среде.

18. Взаимодействие с родителями

18.1. Родители являются ключевыми участниками профилактики цифровых рисков несовершеннолетних.

18.2. Гимназия организует для родителей:
- родительские собрания;
- консультации;
- памятки;
- тематические лекции;
- встречи со специалистами;
- размещение информационных материалов на официальном сайте и иных официальных ресурсах Гимназии.

18.3. Родителям рекомендуется:
- устанавливать понятные семейные правила использования цифровых устройств;
- учитывать возраст ребенка;
- контролировать продолжительность досугового экранного времени;
- не использовать цифровое устройство как постоянную замену общению с ребенком;
- обсуждать с ребенком увиденный им контент;
- знакомить ребенка с правилами защиты персональных данных;
- контролировать возрастную маркировку контента;
- обращать внимание на резкие изменения поведения ребенка после использования социальных сетей и онлайн-игр;
- избегать использования цифровых устройств ребенком непосредственно перед сном;
- обеспечивать регулярную двигательную активность;
- подавать ребенку пример безопасного и умеренного использования цифровых устройств.

18.4. Родителям разъясняется, что рекомендуемые Методическими рекомендациями объемы бытового экранного времени носят профилактический и методический характер, тогда как санитарные требования к использованию ЭСО в образовательной организации являются обязательными в пределах их действия.

19. Просветительская работа

19.1. В течение учебного года Школа организует мероприятия по следующим темам:
- «Безопасность в сети Интернет»;
- «Цифровая гигиена»;
- «Как распознать интернет-мошенника»;
- «Персональные данные и цифровой след»;
- «Кибербуллинг: как защитить себя и помочь другому»;
- «Безопасные социальные сети»;
- «Опасные интернет-челленджи»;
- «Профилактика игровой и интернет-зависимости»;
- «Критическое мышление и проверка информации»;
- «Безопасность онлайн-платежей»;
- «Ответственность за противоправные действия в сети Интернет».

20. Организация мероприятий по внедрению Методических рекомендаций

20.1. Внедрение Методических рекомендаций включает:
- принятие и актуализацию локальных нормативных актов;
- ознакомление педагогических работников с Методическими рекомендациями;
- информирование родителей;
- проведение просветительской работы с обучающимися; анализ организации использования ЭСО;
- оценку цифровых рисков образовательной среды;
- организацию контентной фильтрации;
- включение соответствующих мероприятий в план воспитательной работы;
- повышение квалификации и методическое сопровождение работников;
- проведение внутреннего контроля реализации мероприятий.
20.2. Ответственным за координацию внедрения Методических рекомендаций приказом директора назначается заместитель директора по правовому воспитанию и профилактике правонарушений.
20.3. Ответственное лицо:
- координирует выполнение мероприятий;
- взаимодействует с заместителями директора, педагогом-психологом, классными руководителями, родителями (законными представителями) обучающихся;
- организует мониторинг;
- готовит информационные и аналитические материалы;
- вносит предложения директору по совершенствованию работы.

21. Внутришкольный контроль

21.1. Контроль внедрения настоящего Положения включается в план внутришкольного контроля.
21.2. В рамках контроля изучаются:
- соблюдение продолжительности использования ЭСО;
- организация смены видов деятельности;
- содержание цифровых ресурсов, используемых педагогами;
- проведение профилактических мероприятий;
- работа с родителями;
- функционирование средств контентной фильтрации;
- организация профилактики кибербуллинга;
- исполнение требований по защите персональных данных;
- выполнение Методических рекомендаций с учетом возрастных особенностей обучающихся.
21.3. Формами контроля являются:
- анализ документации;
- посещение учебных занятий;
- мониторинг;
- анкетирование;
- собеседование;
- анализ обращений участников образовательных отношений;
- тематический контроль;
- административный контроль.
21.4. По результатам контроля оформляется:
- справка;
- аналитическая информация;
- приказ директора;
- рекомендации педагогическим работникам;
- план корректирующих мероприятий.

22. Действия при выявлении цифровых рисков

22.1. При получении информации об угрозе жизни или здоровью несовершеннолетнего работник

Гимназии обязан незамедлительно проинформировать администрацию и действовать в соответствии с установленными алгоритмами обеспечения безопасности.
22.2. При выявлении фактов распространения запрещенной информации, противоправного вовлечения несовершеннолетнего, угроз, шантажа либо иных обстоятельств, содержащих признаки правонарушения или преступления, Гимназия действует в пределах своей компетенции и обеспечивает взаимодействие с родителями и уполномоченными органами.
22.3. При выявлении признаков психологического неблагополучия несовершеннолетнего организуется психолого-педагогическое сопровождение в установленном порядке.
22.4. Все действия работников должны осуществляться с соблюдением конфиденциальности и законодательства о персональных данных.

23. Ответственность

23.1. Работники Гимназии несут ответственность за соблюдение требований настоящего Положения в пределах своих должностных обязанностей и в соответствии с законодательством Российской Федерации.
23.2. Нарушение обучающимися требований локальных нормативных актов рассматривается в порядке, установленном законодательством об образовании и Правилами внутреннего распорядка обучающихся.
23.3. Применение мер дисциплинарного воздействия не допускается за действия, за которые законодательством не предусмотрена возможность привлечения обучающегося к дисциплинарной ответственности.

24. Заключительные положения

24.1. Настоящее Положение принимается в порядке, установленном Уставом Гимназии.
24.2. При принятии Положения учитывается мнение Управляющего Совета в порядке, предусмотренном законодательством Российской Федерации и локальными актами Школы.
24.3. Положение вступает в силу со дня его утверждения приказом директора.
24.4. Положение действует до его отмены или принятия нового локального нормативного акта.
24.5. Изменения и дополнения в Положение вносятся при:
- изменении законодательства Российской Федерации;
- изменении санитарных требований;
- утверждении новых федеральных методических рекомендаций;
- выявлении необходимости корректировки порядка организации работы Гимназии.
24.6. Положение размещается на официальном сайте Гимназии.
24.7. Работники Гимназии знакомятся с Положением в установленном порядке.

Приложение 1

Основные возрастные ориентиры профилактической работы

Возрастная группа	Основные цифровые риски	Основные профилактические меры
7–11 лет	Вредный контент, реклама, мошенничество, опасные челленджи, чрезмерное экранное время	Родительский и педагогический контроль, обучение цифровой безопасности, ограничение экранной нагрузки, обсуждение контента
11–16 лет	Кибербуллинг, деструктивные сообщества, интернет-зависимость, манипуляции, распространение личных данных	Развитие критического мышления, цифровой грамотности, обучение способам обращения за помощью, профилактическая работа
16–18 лет	Цифровая репутация, мошенничество, противоправное вовлечение, деструктивный контент, финансовые риски	Осознанное цифровое поведение, правовое просвещение, защита персональных и финансовых данных, развитие медиаграмотности

Приложение 2

План мероприятий по внедрению Методических рекомендаций

№	Мероприятие	Срок	Ответственный	Результат
1	Издание приказа о внедрении Методических рекомендаций	Сентябрь	Директор	Приказ
2	Утверждение настоящего Положения	Сентябрь	Директор	Локальный акт
3	Ознакомление педагогических работников	Сентябрь	Заместитель директора	Лист ознакомления
4	Анализ локальных актов по цифровой и информационной безопасности	Сентябрь	Заместитель директора	Справка
5	Проверка соблюдения требований к использованию ЭСО	1 раз в полугодие	Администрация	Справка ВШК
6	Родительские собрания по вопросам цифровой безопасности	В течение года	Классные руководители	Протоколы
7	Классные часы по цифровой гигиене	В течение года	Классные руководители	Информация
8	Профилактика кибербуллинга	В течение года	Педагог-психолог, заместитель директора по ПВиПП	Отчет
9	Мероприятия по профилактике интернет-мошенничества	В течение года	Заместитель директора по ПВиПП	Справка
10	Мониторинг эффективности внедрения рекомендаций	Май	Администрация	Аналитическая справка

Приложение 3

Памятка обучающемуся «10 правил цифровой безопасности»

1. Не сообщай посторонним свои пароли и коды подтверждения.
2. Не передавай данные банковской карты и иные финансовые сведения.
3. Не переходи по подозрительным ссылкам.
4. Не отправляй незнакомым людям фотографии документов и личные данные.
5. Не соглашайся на личную встречу с интернет-знакомым без ведома родителей.
6. При угрозах, шантаже или травле сохрани доказательства и обратись к взрослому.
7. Проверяй информацию минимум по нескольким надежным источникам.
8. Не участвуй в опасных интернет-челленджах.
9. Соблюдай баланс между цифровой активностью, отдыхом, движением и живым общением.
10. Если происходящее в интернете вызывает страх, тревогу или ощущение опасности, сообщи родителям, классному руководителю, педагогу-психологу или другому взрослому, которому доверяешь.