муниципальное образовательное учреждение средняя общеобразовательная школа
«Образовательный комплекс «Успех» Тутаевского муниципального округа
(МОУ «Образовательный комплекс «Успех»)

ПРИКАЗ

19.12.2025 № 140/01-09
г. Тутаев

**Об обеспечении информационной безопасности
в МОУ «Образовательный комплекс «Успех»**

Руководствуясь Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Концепцией информационной безопасности детей, утвержденной Распоряжением Правительства Российской Федерации от 28.04.2023г. № 1105-р, принимая во внимание методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или)развитию детей, а также не соответствующей задачам образования» (письмо Минпросвещения России от 07.06.2019 №04-474), методические рекомендации об использовании устройств мобильной связи в общеобразовательных организациях (утв. Федеральной службой по надзору прав потребителей и благополучия человека и Федеральной службой по надзору в сфере образования и науки от 14.08.2019г. №№МР 2.4.0150-19/01-230/13-01), в целях обеспечения информационной безопасности в МОУ «Образовательный комплекс «Успех»,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие:
   1.1. Политику информационной безопасности муниципального образовательного учреждения средняя общеобразовательная школа «Образовательный комплекс «Успех» Тутаевского муниципального округа (далее - Политику информационной безопасности) (приложение 1 к настоящему приказу).
   1.2. Правила использования устройств мобильной связи в муниципальном образовательном учреждении средней общеобразовательной школе «Образовательный комплекс «Успех» Тутаевского муниципального округа (приложение 2 к настоящему приказу).
   1.3. Правила использования сети Интернет в муниципальном образовательном учреждении средней общеобразовательной школе «Образовательный комплекс «Успех» Тутаевского муниципального округа (приложение 3 к настоящему приказу).
   1.4. Алгоритм действий педагогических работников МОУ «Образовательный комплекс «Успех» при выявлении противоправного контента в сети интернет (приложение 4 к настоящему приказу).
   1.5. Должностную инструкцию ответственного за организацию доступа к сети интернет и внедрение системы контентной фильтрации МОУ «Образовательный комплекс «Успех» (приложение 5 к настоящему приказу).
2. Назначить ответственными лицами за реализацию Политики информационной безопасности, соблюдение принятого режима безопасности персональных данных и организацию всех мероприятий, направленных на реализацию информационной безопасности в структурных подразделениях следующих руководителей:
   2.1. В Центре образования №3 – Грачёву Н.А.., заместителя директора - руководителя центра образования №3;
   2.2. В Центре образования №7 имени адмирала Ф.Ф. Ушакова – Сапегинну Е.А., заместителя директора - руководителя центра образования №7 имени адмирала Ф.Ф. Ушакова;

2.3. В Центре образования «Емишевский» – Паутову Л.Б., заместителя директора - руководителя центра образования «Емишевский»;

2.4. В Центре образования «Столбищенский» – Кудрявцеву О.Д., заместителя директора - руководителя центра образования «Столбищенский»;

2.5. В Центре образования «Чебаковский» – Родину О.В., заместителя директора - руководителя центра образования «Чебаковский»;

2.6. В Центре развития ребенка - детском саду№4 «Буратино» – Зимину О.А., заместителя директора - руководителя центра развития ребенка - детского сада №4 «Буратино»;

2.7. В Центре развития ребенка - детском саду№6 «Ягодка» –Ледяеву Е.В., заместителя директора - руководителя центра развития ребенка - детского сада №6 «Ягодка»;

2.8. В Центре развития ребенка - детском саду№12 «Полянка» – Касьянову Н.В., заместителя директора - руководителя центра развития ребенка - детского сада №12 «Полянка»;

2.9. В Центре развития ребенка - детском саду№14 «Сказка» – Руденко Р.Г., заместителя директора - руководителя центра развития ребенка - детского сада №14 «Сказка»;

2.10. В Центре развития ребенка - детском саду №22 «Малыш» – Найденову Е.В., заместителя директора - руководителя центра развития ребенка - детского сада №22 «Малыш»;

2.11. В Центре развития ребенка - детском саду№27 «Цветик - семицветик» – Махалову Т.В., заместителя директора - руководителя центра развития ребенка - детского сада №27 «Цветик - семицветик»;

3. Руководителям структурных подразделений ознакомить сотрудников под роспись с положениями Политики информационной безопасности, утвержденной настоящим приказом.

4. Утвердить план мероприятий по обеспечению информационной безопасности обучающихся муниципального образовательного учреждения средняя общеобразовательная школа «Образовательный комплекс «Успех» Тутаевского муниципального округа на 2025-2026 гг. (приложение 6 к настоящему приказу).

5. Контроль исполнения настоящего приказа оставляю за собой.

Директор Е.Е. Сухов

Приложение 1 к приказу
№ 140/01-09 от 19.12.2025

Политика информационной безопасности
муниципального образовательного учреждения средняя общеобразовательная школа «Образовательный комплекс «Успех» Тутаевского муниципального округа

1. Общие положения.

1.1. Политика информационной безопасности муниципального образовательного учреждения средняя общеобразовательная школа «Образовательный комплекс «Успех» Тутаевского муниципального округа (далее соответственно – Политика, Учреждение), разработана в соответствии с требованиями действующего законодательства и нормативных актов Российской Федерации: Федерального закона от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федерального закона от 27 июля 2006 № 152-ФЗ «О персональных данных», Федерального закона от 06 апреля 2011 № 63-ФЗ «Об электронной подписи», Указа Президента Российской Федерации от 06 марта 1997 №188 «Об утверждении Перечня сведений конфиденциального характера», Постановления Правительства РФ №1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства РФ № 687 от 15.09.2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказа Минкомсвязи России от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию», а также ряда иных нормативных правовых актов в сфере защиты информации.

1.2. Политика определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности, которыми руководствуются работники Учреждения при осуществлении своей деятельности.

1.3. Выполнение требований Политики является обязательным для всех работников Учреждения.

1.4. Ответственность за соблюдение информационной безопасности несет каждый работник Учреждения.

2. Цель и задачи Политики информационной безопасности.

2.1. Основными целями Политики являются:

- сохранение конфиденциальности критичных информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам Учреждения;
- защита целостности информации с целью поддержания возможности Учреждения по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Учреждения;
- определение степени ответственности и обязанностей работников по обеспечению информационной безопасности в Учреждении;
- повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз информационной безопасности;
- предотвращение и/или снижение ущерба от инцидентов информационной безопасности.

2.2. Основными задачами Политики являются:

- разработка требований по обеспечению информационной безопасности;
- контроль выполнения установленных требований по обеспечению информационной безопасности;
- повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию информационной безопасности;
- разработка нормативных документов для обеспечения информационной безопасности Учреждения;
- выявление, оценка, прогнозирование и предотвращение реализации угроз информационной

безопасности Учреждения;
- организация антивирусной защиты информационных ресурсов Учреждения;
- защита информации Учреждения от несанкционированного доступа и утечки по техническим каналам связи;
- организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору Учреждения.

3. Концептуальная схема обеспечения информационной безопасности.

3.1. Политика Учреждения направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий работников Учреждения, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

3.2. Наибольшими возможностями для нанесения ущерба обладает собственный персонал Учреждения. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией работников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

3.3. Стратегия обеспечения информационной безопасности Учреждения заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий работников Учреждения.

4. Основные принципы обеспечения информационной безопасности.

Основными принципами обеспечения информационной безопасности являются:
- постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов Учреждения;
- своевременное обнаружение проблем, потенциально способных повлиять на информационную безопасность Учреждения, корректировка моделей угроз и нарушителя;
- разработка и внедрение защитных мер;
- контроль эффективности принимаемых защитных мер;
- персонификация и разделение ролей и ответственности между работниками Учреждения за обеспечение информационной безопасности Учреждения исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5. Объекты защиты.

5.1. Объектами защиты с точки зрения информационной безопасности в Учреждении являются:
- информационный процесс профессиональной деятельности;
- информационные активы Учреждения.

5.2. Защищаемая информация делится на следующие виды:
- информация по финансово - экономической деятельности Учреждения;
- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

6. Требования по информационной безопасности.

6.1. В отношении всех собственных информационных активов Учреждения, активов, находящихся под контролем Учреждения, а также активов, используемых для получения доступа к инфраструктуре Учреждения, должна быть определена ответственность соответствующего работника Учреждения.

6.2. Все работы в пределах Учреждения должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к

использованию в Учреждении.

6.3. Внос в здание и помещения Учреждения личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы Учреждения производится только при согласовании с директором Учреждения.

6.4. Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну Учреждения и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

6.5. В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля. Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким.

6.6. Каждый работник обязан немедленно уведомить директора Учреждения обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети. Доступ третьих лиц к информационным системам Учреждения должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам Учреждения должен быть четко определен, контролируем и защищен.

6.7. Работникам, использующим в работе портативные компьютеры Учреждения, может быть предоставлен удаленный доступ к сетевым ресурсам Учреждения в соответствии с правами в корпоративной информационной системе.

6.8. Работникам, работающим за пределами Учреждения с использованием компьютера, не принадлежащего Учреждению, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

6.9. Работники, имеющие право удаленного доступа к информационным ресурсам Учреждения, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети Учреждения и к каким-либо другим сетям, не принадлежащим Учреждению.

6.10. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Учреждения, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

6.11. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

6.12. Рекомендованные правила:

- работникам Учреждения разрешается использовать сеть Интернет только в служебных целях;
- запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;
- работники Учреждения не должны использовать сеть Интернет для хранения корпоративных данных;
- работа с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Учреждения в сеть Интернет;
- работникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Учреждению;
- работники Учреждения перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть Учреждения для всех лиц, не являющихся работниками Учреждения, включая членов семьи работников Учреждения.

6.13. Директор Учреждения имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

6.14. Работники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация Учреждения.

6.15. Работникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит системный администратор Учреждения.

6.16. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа "мышь", шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей Политики вместе именуются "компьютерное оборудование". Компьютерное оборудование является собственностью Учреждения и предназначено для использования исключительно в производственных целях.

6.17. Каждый работник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

6.18. Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима "Экранной заставки". Для установки режимов защиты пользователь должен обратиться к инженеру-программисту Учреждения. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

6.19. Все программное обеспечение, установленное на компьютерном оборудовании Учреждения, является собственностью Учреждения и должно использоваться исключительно в рабочих целях.

6.20. Работникам Учреждения запрещается устанавливать на предоставленном в пользование компьютерном оборудовании не стандартное, не лицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности.

6.21. На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

- персональный межсетевой экран;
- антивирусное программное обеспечение;
- программное обеспечение шифрования жестких дисков;
- программное обеспечение шифрования почтовых сообщений

6.22. Работники Учреждения недолжны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

6.23. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Работникам запрещается направлять конфиденциальную информацию Учреждения по электронной почте без использования систем шифрования. Строго конфиденциальная информация Учреждения, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

6.24. Использование работниками Учреждения публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации локальной вычислительной сети при условии применения механизмов шифрования.

6.25. Работники Учреждения для обмена документами должны использовать только свой официальный адрес электронной почты.

6.26. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат таком уже утверждению и хранению, что и прочие средства письменных коммуникаций. В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно

проинформировать директора Учреждения. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

6.27. Не допускается при использования электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- рассылка рекламных материалов;
- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам в области этики.

6.28. Объем пересылаемого сообщения по электронной почте не должен превышать 2 Мбайт.

6.29. Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

6.30. В случае кражи переносного компьютера следует незамедлительно сообщить директору Учреждения.

6.31. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения работник обязан:

- про информировать директора и системного администратора Учреждения;
- не пользоваться и не выключать зараженный компьютер; не подсоединять этот компьютер к компьютерной сети Учреждения до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование системным администратором.

6.32. Работникам Учреждения запрещается:

- нарушать информационную безопасность и работу сети Учреждения;
- сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;
- передавать информацию о работниках или списки работников Учреждения посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

6.33. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

6.34. Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

6.35. Только системный администратор Учреждения может создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним по согласованию с директором Учреждения.

6.36. Работники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

6.37. Все заявки на проведение технического обслуживания компьютеров должны направляться системному администратору Учреждения.

6.38. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, и согласованны с системным администратором Учреждения.

7. Управление информационной безопасностью

- Управление информационной безопасностью Учреждения включает в себя:
- разработку и поддержание в актуальном состоянии Политики информационной безопасности;
- разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению информационной безопасности;
- обеспечение бесперебойного функционирования комплекса средств информационной безопасности; осуществление контроля (мониторинга) функционирования системы информационной безопасности;
- оценку рисков, связанных с нарушениями информационной безопасности.

8. Реализация Политики информационной безопасности

Реализация Политики Учреждения осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности.

9. Порядок внесения изменений и дополнений в Политику информационной безопасности

Внесение изменений и дополнений в Политику производится не реже одного раза в три года с целью приведения в соответствие определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

10. Контроль за соблюдением Политики информационной безопасности

Текущий контроль за соблюдением выполнения требований Политики Учреждения возлагается на работника, назначенного приказом директора Учреждения.

Директор Учреждения на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики, а также осуществляет последующий контроль за соблюдением ее требований.

Приложение 2 к приказу
№140/01-09 от 19.12.2025

Правила использования устройств мобильной связи в муниципальном образовательном учреждении средней общеобразовательной школе «Образовательный комплекс «Успех» Тутаевского муниципального округа

1. Общие положения

1.1. Настоящие Правила использования устройств мобильной связи в муниципальном образовательном учреждении средней общеобразовательной школе «Образовательный комплекс «Успех» Тутаевского муниципального округа (далее – Правила) устанавливают порядок использования работниками и обучающимися устройств мобильной связи в зданиях и на территории муниципального образовательного учреждения средняя общеобразовательная школа «Образовательный комплекс «Успех» Тутаевского муниципального округа (далее – Учреждение) в целях профилактики нарушений здоровья обучающихся, повышения эффективности образовательного процесса, а также защиты гражданских прав всех участников образовательных отношений.

1.2. Настоящие Правила разработаны в соответствии с:

- Конституцией Российской Федерации,
- Федеральным законом от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации",
- Федеральным законом от 19.12.2023 № 618-ФЗ «О внесении изменений в Федеральный закон «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 24.07.1998 № 124-ФЗ "Об основных гарантиях прав ребенка в Российской Федерации",
- 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 14.08.2019 г.
- Постановлением главного государственного санитарного врача РФ от 28.09.2020г. №28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно- эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи»,
- иными нормативными правовыми актами, действующими на территории РФ.

1.3. Соблюдение настоящих Правил обеспечивает:

- реализацию права каждого обучающегося на получение образования в соответствии с федеральными государственными образовательными стандартами при реализации прав и свобод других лиц,
- уменьшение вредного воздействия радиочастотного и электромагнитного излучения средств мобильной связи на участников образовательных отношений,
- защиту обучающихся от пропаганды насилия, жестокости, порнографии и другой информации, причиняющей вред их здоровью и развитию,
- повышение уровня дисциплины.

1.4. Настоящие Правила размещаются на официальном сайте Учреждения в сети Интернет.

2. Условия применения средств мобильной связи

2.1. Не допускается использование средств подвижной радиотелефонной связи во время проведения учебных занятий при освоении основных и адаптированных общеобразовательных программ, за исключением случаев возникновения угрозы жизни или здоровью обучающихся, работников Учреждения, иных экстренных случаев.

2.2. Не рекомендуется пользование мобильной связью до начала уроков, на переменах.

2.3. До урока и внеурочных мероприятий (на период образовательного процесса):

– следует отключить и убрать все технические устройства (плееры, наушники, гаджеты, планшеты, телефоны, различные записные устройства и пр.),

– отключить мобильный телефон и (или) перевести в режим «без звука»,

– убрать мобильный телефон и (или) другие технические устройства со стола.

2.4. Средства мобильной связи, в т.ч. в выключенном состоянии, не должны находиться на партах в классах и на обеденных столах в столовой.

2.5. Родителям (законным представителям) обучающихся не рекомендуется звонить своим детям во время образовательного процесса. В случае необходимости они могут позвонить на перемене, ориентируясь на расписание звонков, размещенное на сайте Учреждения. В случае форс-мажорных обстоятельств для связи со своими детьми во время образовательного процесса родителям (законным представителям) рекомендуется передавать сообщения через делопроизводителя Учреждения по телефонам, размещенным на сайте Учреждения.

2.6. При использовании на перемене средств мобильной связи необходимо соблюдать следующие этические нормы:

– не следует использовать в качестве звонка мелодии и звуки, которые могут оскорбить или встревожить окружающих;

– разговаривать с собеседником нужно максимально тихим голосом;

– не следует вести приватные разговоры с использованием средств мобильной связи в присутствии других людей;

– недопустимо использование чужих средств мобильной связи и сообщение их номеров третьим лицам без разрешения на то владельцев.

2.7. При входе в Учреждение перевести устройства мобильной связи в режим «без звука» (в том числе с исключением использования режима вибрации из-за возникновения фантомных вибраций).

2.8. Ответственность за сохранность средств мобильной связи лежит только на его владельце (родителях, законных представителях владельца).

Все случаи хищения имущества рассматриваются в установленном законом порядке и преследуются в соответствии с законодательством РФ.

2.9. 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, индивидуальных шкафчиках, в раздевалках спортзала.

2.10. Всем участникам образовательных отношений пользоваться памяткой для обучающихся, родителей и педагогических работников по профилактике неблагоприятных для здоровья и обучения детей эффектов от воздействия устройств мобильной связи (Приложение к Правилам).

2.11. Все спорные вопросы между участниками образовательных отношений в отношении соблюдения настоящих Правил разрешаются путем переговоров с участием представителей администрации, директора Учреждения и Комиссии по урегулированию споров между участниками образовательных отношений.

3. Права и обязанности пользователей мобильной связи

3.1. Пользователи мобильной связи при выполнении указанных в разделе 2 требований имеют право в свободное от учебных занятий время:

– осуществлять и принимать звонки;

– получать и отправлять SMS и MMS;

– прослушивать аудиозаписи (с использованием наушников);

– просматривать видео сюжеты (с использованием наушников);

3.2. Фото-и видеосъемка лиц, находящихся в Учреждении, производится только с их согласия.

3.3. Пользователи обязаны помнить о том, что согласно Конституции Российской Федерации:

– осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц (п. 3 ст. 17);

– сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (п. 1 ст. 24).

4. Ответственность за нарушение Правил

4.1. За нарушение настоящих Правил пользователи средств мобильной связи несут ответственность в соответствии с действующим законодательством Российской Федерации,

Уставом и локальными нормативными актами Учреждения.

4.2. За однократное нарушение педагогический работник Учреждения должен сделать обучающемуся замечание и довести факт нарушения настоящих Правил в виде докладной записки до сведения руководителя структурного подразделения (с написанием объяснительной обучающегося).

5. Срок действия Правил

5.1. Настоящие Правила вступают в силу с момента утверждения приказом директора Учреждения и действуют до внесения изменений и дополнений в Правила или утверждения новых Правил.

Приложение к правилам использования
устройств мобильной связи

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 2метров от головы.

Приложение 3 к приказу
№140/01-09 от 19.12.2025

Правила использования сети Интернет
в муниципальном образовательном учреждении средней общеобразовательной школе «Образовательный комплекс «Успех» Тутаевского муниципального округа

1. **Общие положения**

1.1. Настоящие Правила использования сети Интернет в муниципальном образовательном учреждении средней общеобразовательной школе «Образовательный комплекс «Успех» Тутаевского муниципального округа (далее – Правила) регулируют порядок и условия использования сети Интернет через ресурсы муниципального образовательного учреждения средняя общеобразовательная школа «Образовательный комплекс «Успех» Тутаевского муниципального округа (далее – Учреждение) обучающимися и работниками.

1.2. Использование сети Интернет в Учреждении направлено на решение задач образовательного процесса.

1.3. Настоящие Правила имеют статус локального нормативного акта Учреждения. Если нормами действующего законодательства Российской Федерации предусмотрены иные требования, чем настоящими Правилами, применяются нормы действующего законодательства Российской Федерации.

1.4. Ознакомление с Правилами и соблюдение их обязательны для всех обучающихся и работников Учреждения, а также иных лиц, допускаемых к работе с ресурсами и сервисами сети Интернет Учреждения.

2. **Организация использования сети Интернет в Учреждении**

2.1. Еженедельный мониторинг использования сети Интернет участниками образовательного процесса осуществляет системный администратор Учреждения в соответствии с настоящими Правилами.

2.2. Доступ к ресурсам, несовместимыми с целями и задачами образования и воспитания, запрещен.

2.3. При использовании сети Интернет в Учреждении обучающимися, учителями и иными работниками предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношение к образовательному процессу.

2.4. Использование сети Интернет обучающимися допускается только с разрешения учителя. Учитель, давший обучающемуся разрешение на работу в сети Интернет, несет ответственность за соблюдение обучающимся настоящих Правил наравне с ним.

2.5. Во время учебных и других занятий в рамках образовательного процесса контроль использования обучающимися сети Интернет осуществляет учитель, ведущий занятие:

– наблюдает за использованием компьютера в сети Интернет обучающимися;

– принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу;

– сообщает ответственному за информатизацию о преднамеренных попытках обучающегося осуществить доступ к ресурсам, не совместимыми с задачами образования.

2.6. В свободное время использование обучающимися и иными лицами сети Интернет допускается по расписанию кабинетов, оборудованных компьютерами, в присутствии учителя.

2.7. Работники Учреждения, имеющие рабочее место, оборудованное компьютером с подключением к сети Интернет, используют сеть в любое время в рамках режима работ

Учреждения в соответствии с п. 2.3 настоящих Правил.

2.8. При использовании сетевых сервисов, предполагающих авторизацию, запрещается пользоваться чужими учетными данными.

2.9. Все компьютеры, подключаемые к сети Интернет, обязаны иметь установленное, действующее и обновляющееся антивирусное программное обеспечение.

3. Права, обязанности и ответственность пользователей

3.1. Использование ресурсов сети Интернет в Учреждении осуществляется в целях образовательного процесса.

3.2. Работники и обучающиеся могут бесплатно пользоваться доступом к глобальным Интернет-ресурсам.

3.3. Пользователям запрещается:

– посещать сайты, содержание и тематика которых недопустимы для несовершеннолетних и (или) нарушают законодательство Российской Федерации (порнография, эротика, пропаганда насилия, терроризма, политического и религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);

– загружать и распространять материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, а также размещение ссылок на выше указанную информацию;

– загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

– распространять информацию, порочащую честь и достоинство граждан;

– осуществлять любые сделки через сеть Интернет;

– работать с объемными ресурсами (видео, аудио, чат, фото) без согласования с учителем.

3.4. Пользователи имеют право:

– работать в сети Интернет в течение периода времени, в рамках режима работы Учреждения;

– сохранять полученную информацию на съемном носители.

3.5. Пользователи несут ответственность:

– за содержание передаваемой, принимаемой и печатаемой информации;

– за нанесение любого ущерба оборудованию (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность в соответствии с законодательством.

Приложение 4 к приказу
№140/01-09 от 19.12.2025

Алгоритм действий педагогических работников
«Образовательный комплекс «Успех»
при выявлении противоправного контента в сети«Интернет»

В случае выявления в сети «Интернет» информации, распространение которой запрещено на территории Российской Федерации, необходимо направить сообщение о распространении на странице сайта в сети «Интернет» такого контента (далее – Сообщение).

1. Для направления ссылок на сайты или страницы сайтов в сети «Интернет», содержащие материалы с признаками запрещенной информации, посредством электронной формы необходимо выполнить следующие действия:

- открыть посредством интернет-браузера раздел сайта Роскомнадзора «*Единый реестр запрещенной информации*» (https://eais.rkn.gov.ru/). В подразделе «*Прием сообщений*» (http://eais.rkn.gov.ru/feedback/) сформировать Сообщение о наличии на сайте или странице сайта в сети «Интернет» признаков запрещенной информации (поля, отмеченные знаком «*» обязательны для заполнения);

- в поле «*Тип информации*» следует выбрать один из типов запрещенного к распространению контента;

- ввести в поле «*Указатель страницы сайта в сети «Интернет*» конкретную ссылку на интернет-страницу сайта в сети «Интернет» (например, http://example.com/example.html), где содержатся признаки запрещенной информации;

- в подразделе «*Заявитель*» в полях «*Фамилия*», «*Имя*», «*Отчество*», «*Место работы*» имеется возможность указать соответствующие данные должностного лица, направившего Сообщение и наименование Органа;

- в поле «*E-mail*» следует указать активный адрес электронной почты для получения уведомления о результатах отработки Сообщения. На указанный адрес электронной почты будут направляться уведомления о принятии ссылок к рассмотрению и о включении их в Единый реестр.

2. В Сообщении следует указывать конкретную страницу интернет-сайта, содержащую признаки наличия запрещенной информации.

В Сообщении не следует указывать ссылки на результаты поисковых запросов поисковых систем в сети «Интернет» (например, https://yandex.ru/search..., https://www.google.ru/… и т.д.), а также ссылки на результаты поисковых запросов поисковых сервисов интернет-сайтов (например, http://vk.com/search...).

Внесение в Единый реестр указателей страниц сайтов поисковых систем в сети «Интернет» приведет к ограничению доступа именно к поисковым сервисам, а не к ресурсам, содержащим запрещенную информацию.

Кроме того, результаты поисковых запросов, отображаемых поисковыми сервисами интернет-сайтов и непосредственно поисковыми системами в сети «Интернет», могут меняться в зависимости от релевантности запрашиваемой информации, что не позволяет точно идентифицировать страницу сайта в сети «Интернет», на которой размещен запрещенный материал.

В случае выявления с помощью вышеуказанных поисковых сервисов интернет-сайтов и поисковых систем в сети «Интернет» запрещенной информации, следует установить конкретный адрес страницы сайта в сети «Интернет», на котором данный материал размещен (перейдя по ссылке, отображаемой поисковым интернет-сервисом), и сформировать посредством электронной формы Сообщение в порядке, установленном настоящим Алгоритмом.

3. Электронная форма, опубликованная на сайте в сети «Интернет» http://blocklist.rkn.gov.ru, позволяет получить данные о принятых мерах по ограничению доступа к сайтам и (или) страницам сайтов сети «Интернет» в рамках исполнения требований статей 15.1–15.6-1 и 15.8 Федерального закона № 149-ФЗ.

Для этого в указанной электронной форме следует ввести данные об указателе страницы сайта в сети «Интернет» или доменном имени интернет-ресурса с обязательным указанием протокола передачи данных («http://» или «https://» в зависимости от того, какой протокол передачи данных использует интернет-ресурс).

Приложение 5 к приказу
№140/01-09 от 19.12.2025

Должностная инструкция
ответственного за организацию доступа к сети интернет и внедрение системы контентной фильтрации МОУ «Образовательный комплекс «Успех»

1. **Общие положения**

Должен знать:

- дидактические возможности использования ресурсов сети Интернет;
- правила безопасного использования сети Интернет;
- методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

2. **Должностные обязанности:**

- планирует использование ресурсов сети интернет в образовательном учреждении на основании заявок преподавателей и других работников лицея;
- разрабатывает, согласует с педагогическим коллективом, представляет на педагогическом совете лицея локальные нормативные акты образовательной организации в сфере обеспечения информационной безопасности детей;
- организует получение сотрудниками электронных адресов и паролей для работы в сети интернет и информационной среде образовательного учреждения;
- организует контроль использования сети интернет в образовательном учреждении;
- организует контроль работы оборудования и программных средств, обеспечивающих использование Реестра безопасных образовательных сайтов в образовательной организации;
- организует контроль реализации в образовательном учреждении методических рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;
- систематически повышает свою профессиональную квалификацию по направлению
- «Организация защиты детей от видов информации, распространяемой посредством сети интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательных организациях»;
- обеспечивает информирование организаций, отвечающих за работу технических и программных средств, об ошибках в работе оборудования и программного обеспечения;
- соблюдает правила и нормы охраны труда, техники безопасности и противопожарной защиты, правила использования сети интернет.

3. **Права**

Вправе осуществлять действия организационно-административного характера для обеспечения ограничения доступа обучающихся к видам информации, распространяемой посредством сети интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательной организации.

4. **Ответственность**

Несет ответственность за ограничение доступа обучающихся к видам информации, распространяемой посредством сети интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательной организации.

Приложениебкприказу
№140/01-09 от 19.12.2025

План мероприятий
по обеспечению информационной безопасности обучающихся муниципального образовательного учреждения средняя общеобразовательная школа «Образовательный комплекс «Успех» Тутаевского муниципального округа
на 2025-2026 гг.

№	Мероприятие	Сроки	Ответственный
1.	Актуализация локальной нормативной документации МОУ«Образовательный комплекс «Успех», обеспечивающей защиту информации и обеспечение информационной безопасности	Январь-февраль, в течение года по мере необходимости	Ответственный за обеспечение информационной безопасности
2.	Организация контроля за обеспечением защиты детей от распространения информации, причиняющей вред их здоровью и развитию в соответствии с действующим законодательством.	Постоянно	Ответственный за обеспечение информационной безопасности
3.	Организация контроля за соблюдением законодательства РФ о защите детей от информации, причиняющей вред их здоровью и развитию: - рассмотрение в срок, не превышающий десяти рабочих дней со дня получения, обращений, жалоб о нарушениях законодательства РФ о защите детей от информации, причиняющей вред их здоровью и развитию, включая несоответствие применяемых административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и развитию, а также о наличии доступа детей к информации, запрещенной для распространения среди детей, и направление мотивированного ответа о результатах рассмотрения таких обращений, жалоб или претензий; - установление в течение десяти рабочих дней со дня получения обращений, жалоб или претензий о наличии доступа детей к информации, запрещенной для распространения среди детей, причин и условий возникновения такого доступа и принятие мер по их устранению.	Постоянно	Ответственный за обеспечение информационной безопасности
4.	Актуализация раздела «Информационная безопасность» на официальном сайте МОУ «Образовательный комплекс «Успех», публикация материалов по обеспечению информационной безопасности детей при использовании ресурсов сети Интернет.	В течение года по мере необходимости	Ответственный за обеспечение информационной безопасности
5.	Проверка работоспособности системы контентной фильтрации в МОУ «Образовательный комплекс«Успех».	Ежемесячно	Системный администратор

6.	Обеспечение эффективного функционирования антивирусной защиты компьютерной техники, имеющей доступ к сети Интернет.	Постоянно	Системный администратор
7.	Функционирование контент - фильтра в МОУ «Образовательный комплекс «Успех». Организация контроля по ограничению доступа к информационной продукции, информации, причиняющей вред здоровью и (или) развитию детей.	Постоянно	Системный администратор
8.	Контроль безопасности содержания приобретаемой информационной продукции для обучающихся в соответствии с возрастными категориями.	По мере приобретения	Заведующий библиотекой
9.	Рассмотрение вопросов обеспечения информационной безопасности обучающихся при использовании ресурсов сети Интернет на педагогических советах лицея.	По графику проведения педагогических советов	Ответственный за обеспечение информационной безопасности
10.	Ознакомление работников МОУ «Образовательный комплекс «Успех» с методическими рекомендациями по ограничению в образовательных учреждениях доступа обучающихся к видам информации, распространяемой посредством сети интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, и локальными нормативными актами МОУ «Образовательный комплекс «Успех» по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет.	При приеме на работу новых работников	Ответственный за обеспечение информационной безопасности
11.	Ознакомление работников МОУ «Образовательный комплекс «Успех» с сайтами в сети интернет, включенных в Реестр безопасных образовательных сайтов	При приеме на работу новых работников	Ответственный за обеспечение информационной безопасности
12.	Информирование работников МОУ «Образовательный комплекс «Успех», обучающихся и их родителей (законных представителей) об ответственности за нарушение требований законодательства Российской Федерации и организационно-распорядительных документов образовательной организации по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет.	Август - сентябрь	Ответственный за обеспечение информационной безопасности
13.	Информирование родителей (законных представителей) обучающихся о существующих угрозах в сети Интернет, о методах и способах защиты детей от информации, причиняющей вред здоровью и (или) развитию детей. Организация профилактических мероприятий по вопросам информационной безопасности.	По плану проведения классных часов и родительских собраний	Классные руководители. Социальный педагог.
14.	Организация преподавания обучающимся основ информационной безопасности в рамках	В течение Учебного года	Ответственный за обеспечение

	реализации рабочей программы учебного предмета «Информатика».		информационной безопасности
15.	Проведение Единого урока по безопасности в сети интернет.	Сентябрь-октябрь	Учителя информатики
16.	Проведение Всероссийской контрольной работы по информационной безопасности *на сайте www.Единыйурок.дети*	Октябрь-ноябрь	Учителя информатики
17.	Оформление и обновление стендов «Информационная безопасность» *в соответствии с письмом Минобрнауки России от 14.05.2018 №08-1184 «О направлении информации»*	В течение учебного года	Ответственный за обеспечение информационной безопасности
18.	Прохождения педагогическими и иными работниками МОУ «Образовательный комплекс«Успех» программы повышения квалификации на сайте Единыйурок.рф по направлению «Безопасное использование сайтов в сети интернет в образовательном процессе в целях обучения и воспитания обучающихся в образовательной организации».	Раз в два календарных года	Ответственный за обеспечение информационной безопасности
19.	Использование в работе образовательных программ, направленных на формирование навыков у обучающихся, их родителей и педагогических работников безопасного поведения в информационной среде, рекомендованных Экспертным советом по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества.	В течение учебного года	Ответственный за обеспечение информационной безопасности