Государственное бюджетное общеобразовательное учреждение Самарской области
средняя общеобразовательная школа с. Герасимовка
муниципального района Алексеевский Самарской области

СОГЛАСОВАНО
Управляющим советом
ГБОУ СОШ с. Герасимовка
Протокол № 1 от «28» августа 2026г.

УТВЕРЖДАЮ
Директор ГБОУ СОШ с. Герасимовка
_____ /Н.А. Саяпина/
Приказ № 370 от «28» августа 2026г.

# Положение
# об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования

ПРИНЯТО
педагогическим советом
ГБОУ СОШ с. Герасимовка
Протокол № 1 от 28.08.2026г.

ПРИНЯТО с учётом мнения Совета обучающихся
Протокол № 1 от 28.08.2026г.

Подписано цифровой подписью:
Саяпина Н.А.
DN: c=RU, o=ГБОУ СОШ с. Герасимовка, cn=Саяпина Н.А., email=uv.geras_sch@63edu.ru
Дата: 2026.10.27 09:27:18 +04'00'

## 1. Общие положения

1.1. Настоящее Положение регулирует условия и порядок использования сети «Интернет» в государственном бюджетном общеобразовательном учреждении Самарской области средней общеобразовательной школе с. Герасимовка муниципального района Алексеевский Самарской области (далее — Школа).

1.2. Использование сети «Интернет» в Школе направлено на решение задач учебно-воспитательного процесса.

1.3. Положение имеет статус локального нормативного акта Школы и обязательно для исполнения всеми работниками, обучающимися и иными участниками образовательных отношений.

1.4. Положение разработано в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в том числе ст. 15.1);
- 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»;
- приказом 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» (в действующей редакции приказа Минцифры России от 25.03.2025 № 234);
- Методическими рекомендациями 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);
- письмом Минпросвещения России от 24.08.2021 № 04-ПГ-МП-30120 «О применении Методических рекомендаций по ограничению в образовательных организациях доступа обучающихся к видам информации...»;
- планом мероприятий (дорожной картой) по обеспечению информационной безопасности детей на 2021–2027 годы, утверждённым приказом Минцифры России от 01.12.2020 № 644;
- требованиями к подключению образовательных организаций к единой сети передачи данных (приказ Минцифры России и Минпросвещения России от 30.04.2021 № 417/221 в редакции приказа от 31.08.2022 № 634/789);
- Правилами оказания услуг связи по передаче данных (постановление Правительства РФ от 31.12.2021 № 2606) и Правилами оказания телематических услуг связи (постановление Правительства РФ от 31.12.2021 № 2607);
- распоряжениями Правительства РФ от 23.01.2024 № 121-р и от 26.12.2024 № 4039-р, распоряжением Президента РФ от 29.12.2025 № 519-рп;
- действующими государственными контрактами на оказание услуг связи для образовательных организаций.

1.5. Доступ Школы к сети «Интернет» осуществляется с использованием единой сети передачи данных (далее — ЕСПД), услуги по организации и защите которой оказываются ПАО «Ростелеком» на основании действующих государственных контрактов, заключённых уполномоченным органом Самарской области. В соответствии с распоряжением Президента Российской Федерации от 29.12.2025 № 519-рп закупка услуг связи для государственных и муниципальных образовательных организаций в 2026–2027 годах осуществляется уполномоченными органами субъектов Российской Федерации.

## 2. Термины и сокращения

*СКФ* — система контентной фильтрации, обеспечивающая ограничение доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

*ЕСПД* — единая сеть передачи данных, через которую образовательным организациям предоставляется доступ к сети «Интернет» с контентной фильтрацией.

*АРМ* — автоматизированное рабочее место (компьютер) с доступом к сети «Интернет».
Единый реестр — Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.
*РБОС* — Перечень сайтов в сети «Интернет», рекомендованных и одобренных для использования в образовательном процессе (Реестр безопасных образовательных сайтов).
*Негативная информация* — виды информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.
*«Чёрный список»* — контентная фильтрация и ограничение доступа обучающихся к информации, включённой в перечень видов негативной информации.
*«Белый список»* — контентная фильтрация и предоставление доступа обучающимся только к сайтам, включённым в РБОС.
*Совет* — Совет по обеспечению информационной безопасности обучающихся в Школе.

## 3. Организация использования сети «Интернет» в Школе

3.1. Вопросы использования возможностей сети «Интернет» в учебно-воспитательном процессе рассматриваются на Педагогическом совете Школы. Педагогический совет утверждает Правила использования сети «Интернет» на учебный год; Правила вводятся в действие приказом директора Школы.

3.2. Директор Школы отвечает за обеспечение эффективного и безопасного доступа к сети «Интернет», а также за выполнение установленных Правил.

3.3. Для организации доступа участников образовательных отношений к сети «Интернет» в соответствии с установленными Правилами директор Школы приказом назначает ответственного за организацию работы с сетью «Интернет» и ограничение доступа (далее — Ответственный).

3.4. Ответственный:

- организует работу СКФ и обеспечивает её бесперебойное функционирование;
- ведёт журнал работы СКФ;
- взаимодействует с технической поддержкой ЕСПД, работает в личном кабинете ЕСПД (направление заявок на блокирование и разблокирование ресурсов, управление настройками фильтрации);
- принимает решение о разрешении/блокировании доступа к определённым ресурсам и (или) категориям ресурсов в пределах своей компетенции;
- фиксирует выявленные случаи обращения обучающихся к негативной информации и принимает меры реагирования;
- осуществляет действия организационно-административного характера для обеспечения ограничения доступа обучающихся к негативной информации.

3.5. В Школе действует Совет по обеспечению информационной безопасности обучающихся (далее — Совет), который рассматривает вопросы организации работы СКФ, реализации Методических рекомендаций и плана мероприятий (Приложение 2), а также заслушивает отчёты Ответственного. Решения о разрешении/блокировании доступа к определённым ресурсам и (или) категориям ресурсов сети «Интернет» принимаются Педагогическим советом Школы.

3.6. Во время уроков и других занятий в рамках учебного плана контроль использования обучающимися сети «Интернет» осуществляет педагогический работник, ведущий занятие. Во время свободного доступа обучающихся к сети «Интернет» вне учебных занятий контроль осуществляют работники Школы, определённые приказом директора.

## 4. Система контентной фильтрации

4.1. СКФ реализуется на базе ЕСПД, предоставляемой ПАО «Ростелеком». Настройку и актуализацию режимов контентной фильтрации осуществляет оператор связи в рамках исполнения действующих государственных контрактов.

4.2. ЕСПД обеспечивает: передачу данных по защищённым каналам связи; блокирование доступа к ресурсам из Единого реестра и к ресурсам с информацией, запрещённой или ограниченной к распространению среди детей; антивирусную защиту трафика; мониторинг каналов связи.

4.3. Технология контентной фильтрации не должна меняться чаще одного раза в год.

4.4. СКФ обеспечивает: безопасный поиск; ведение статистики обращений к ресурсам сети «Интернет»; автоматическое обновление правил фильтрации с учётом перечня РБОС не позднее 3 рабочих дней.

4.5. Отключение СКФ не допускается без письменного согласия директора Школы. Снятие фильтрации с отдельных АРМ (административно-хозяйственных, не используемых обучающимися) допускается только на основании письменного распоряжения директора и заявки через личный кабинет ЕСПД либо обращения в Ситуационный центр Минцифры России (телефон: 8 (800) 301-34-14). С АРМ, используемых обучающимися, контентная фильтрация не снимается.

4.6. В случае блокирования ресурса, необходимого для образовательного процесса, педагогический работник сообщает об этом Ответственному. Ответственный проверяет ресурс на соответствие задачам образования и направляет заявку на разблокирование через личный кабинет ЕСПД либо в техническую поддержку ЕСПД. До принятия решения доступ к ресурсу не предоставляется.

4.7. Ответственный ведёт журнал работы СКФ, в котором фиксируются: дата и время события; доменный адрес ресурса; характер события (блокирование, разблокирование, сбой, заявка); принятые меры. Журнал хранится у Ответственного и предъявляется по требованию директора и органов управления образованием.

4.8. Не реже одного раза в учебную четверть Ответственный проводит проверку качества работы СКФ (тестирование по единым правилам, анализ статистики обращений). Ежегодно, до начала учебного года, проводится мониторинг эффективности СКФ в порядке, установленном разделом 5 настоящего Положения, с оформлением акта по форме согласно Приложению № 3.

## 5. Порядок проведения проверки эффективности использования СКФ

5.1. Проверка эффективности использования СКФ проводится в Школе в целях подтверждения соответствия СКФ требованиям Методических рекомендаций и приказу Минкомсвязи России от 16.06.2014 № 161 (в действующей редакции), а также своевременного выявления и устранения недостатков контентной фильтрации.

5.2. Проверки проводятся:

- ежегодно, до 30 августа, — в рамках ежегодного мониторинга качества работы СКФ с отчётом на Педагогическом совете Школы до начала учебного года;
- ежеквартально — Ответственным и Советом в рамках периодического контроля;
- внепланово — по поручению директора Школы, при обращениях педагогических работников о неэффективной работе СКФ, а также по требованию органов управления образованием и надзорных органов.

5.3. Для проведения ежегодной проверки директор Школы приказом создаёт комиссию. В состав комиссии включаются: заместитель директора (председатель комиссии), Ответственный, представитель Совета. Комиссия вправе привлекать педагогических работников, преподающих информатику, и специалистов, обслуживающих компьютерное оборудование Школы.

5.4. В ходе проверки комиссия и Ответственный проверяют:

- работоспособность СКФ на всех АРМ Школы и в сетях Wi-Fi;
- блокирование доступа к ресурсам, включённым в Единый реестр, и к ресурсам с информацией из Приложения № 1 к настоящему Положению (методом тестовых обращений к контрольным ресурсам и проверки отображения специальной страницы блокировки);
- принудительное включение безопасного поиска в используемых поисковых системах;
- ведение и доступность статистики обращений к ресурсам сети «Интернет», в том числе заблокированных;
- актуальность правил фильтрации с учётом РБОС (обновление не позднее 3 рабочих дней после изменения перечня);
- ведение журнала работы СКФ (Приложение № 4 к настоящему Положению) и полноту фиксации в нём событий;
- отсутствие отключений СКФ на АРМ, используемых обучающимися;

- функционирование идентификации пользователей при подключении через сети Wi-Fi (раздел 6 настоящего Положения).

5.5. Результаты проверки оформляются актом по форме согласно Приложению № 3 к настоящему Положению. Акт подписывается председателем и членами комиссии и хранится у Ответственного.

5.6. При выявлении недостатков (необоснованное блокирование ресурсов, необходимых для образовательного процесса; отсутствие блокирования негативной информации; неработающий безопасный поиск) Ответственный направляет заявку в личный кабинет ЕСПД либо в техническую поддержку ПАО «Ростелеком» и контролирует её исполнение. О результатах устранения недостатков комиссия информирует директора Школы.

5.7. Результаты ежегодной проверки доводятся до сведения Педагогического совета Школы и учитываются при актуализации плана мероприятий (Приложение № 2 к настоящему Положению).

## 6. Использование Wi-Fi и идентификация пользователей

6.1. Точки доступа Wi-Fi приравниваются к пунктам коллективного доступа в сети «Интернет». Анонимный доступ к сети «Интернет» через Wi-Fi в Школе не допускается.

6.2. Идентификация пользователей осуществляется одним из следующих способов (п. 28 Правил № 2606): предъявлением документа, удостоверяющего личность; через учётную запись в единой системе идентификации и аутентификации (ЕСИА, портал Госуслуг); с использованием абонентского номера мобильного телефона. Авторизация с использованием учётных записей в социальных сетях не применяется.

6.3. При подключении к гостевой сети Wi-Fi пользователь автоматически перенаправляется на страницу идентификации, предоставляемую оператором связи (ПАО «Ростелеком»). До прохождения идентификации доступ к сети «Интернет» не предоставляется.

6.4. В Школе создаются три раздельные сети Wi-Fi: для обучающихся (изолированная от административной сети); для работников; гостевая. Объединение указанных сетей между собой не допускается.

6.5. Подключение личных устройств обучающихся к Wi-Fi Школы осуществляется в порядке, установленном приказом директора, при наличии согласия родителей (законных представителей) несовершеннолетних обучающихся.

6.6. При персональной идентификации обучающегося доступ предоставляется с учётом возрастной классификации информационной продукции по Федеральному закону № 436-ФЗ. При отсутствии персональной идентификации доступ предоставляется только к информации с возрастной категорией «6+».

6.7. Ответственный ведёт учёт подключений к Wi-Fi (MAC-адрес устройства, идентификатор пользователя, дата и время подключения) и реестр точек доступа. Пароли сетей Wi-Fi изменяются не реже одного раза в год, а также при их компрометации.

6.8. Запрещаются: подключение к сети Школы личных (не принадлежащих Школе) маршрутизаторов и точек доступа; раздача сети «Интернет» с личных устройств обучающихся в обход СКФ. При обнаружении несанкционированной точки доступа Ответственный немедленно отключает её, фиксирует факт в журнале СКФ и докладывает директору.

## 7. Контроль за использованием сети «Интернет»

7.1. Лицо, осуществляющее контроль за использованием обучающимися сети «Интернет»:

- определяет время и место работы обучающихся в сети «Интернет» с учётом технических возможностей Школы, а также длительность сеанса работы каждого обучающегося;
- наблюдает за использованием обучающимися компьютеров и сети «Интернет»;
- способствует осуществлению контроля объёмов трафика;
- запрещает дальнейшую работу обучающегося в сети «Интернет» на уроке (занятии) в случае нарушения им порядка использования сети «Интернет»;
- доводит до классного руководителя информацию о нарушении обучающимся Правил работы в сети «Интернет»;

- принимает необходимые меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

## 8. Порядок осуществления контроля педагогическими работниками использования обучающимися сети «Интернет»

8.1. Во время уроков и других занятий в рамках учебного плана контроль использования обучающимися сети «Интернет» осуществляет педагогический работник, ведущий занятие. Педагогический работник:

- организует работу обучающихся в сети «Интернет» в соответствии с образовательной программой и определяет перечень ресурсов, используемых на занятии;
- наблюдает за использованием обучающимися компьютеров и сети «Интернет»;
- принимает меры по пресечению обращений к ресурсам, содержащим негативную информацию;
- запрещает дальнейшую работу обучающегося в сети «Интернет» в случае нарушения им Правил использования сети «Интернет» и информирует классного руководителя.

8.2. Во время свободного доступа обучающихся к сети «Интернет» вне учебных занятий контроль осуществляют работники Школы, назначенные приказом директора.

8.3. Педагогические работники и иные контролирующие работники не оставляют обучающихся без присмотра при работе с АРМ, имеющими доступ к сети «Интернет».

8.4. При обнаружении ресурса с негативной информацией педагогический работник действует в порядке, установленном разделом 10 настоящего Положения: фиксирует доменный адрес ресурса и время его обнаружения, незамедлительно сообщает Ответственному.

8.5. О преднамеренных попытках обучающегося обратиться к ресурсам с негативной информацией педагогический работник информирует классного руководителя; классный руководитель при необходимости информирует родителей (законных представителей) обучающегося.

8.6. Педагогические работники знакомят обучающихся с инструкцией по обеспечению информационной безопасности при использовании сети «Интернет» (Приложение № 5 к настоящему Положению), размещённой в учебных кабинетах: обязательно в начале учебного года и далее не реже одного раза в учебную четверть.

8.7. Классные руководители проводят информирование родителей (законных представителей) об угрозах в сети «Интернет» и об ответственности за нарушение требований законодательства в рамках родительских собраний (Приложение № 2 к настоящему Положению).

## 9. Права и обязанности обучающихся

9.1. Обучающиеся имеют доступ к ресурсам сети «Интернет» согласно режиму работы Школы.

9.2. Обучающиеся должны воздерживаться от любых действий, способных причинить вред информационным ресурсам Школы, программному и аппаратному обеспечению компьютеров.

9.3. Обучающиеся используют сеть «Интернет» в Школе исключительно в целях образовательного процесса.

9.4. Обучающиеся должны осознавать, что технические средства и программное обеспечение не обеспечивают полную фильтрацию ресурсов сети «Интернет», и в связи с этим осознают возможную опасность столкновения с ресурсом, содержание которого противоречит законодательству Российской Федерации и несовместимо с целями и задачами образовательного процесса.

9.5. Обучающемуся запрещается:

- обращаться к ресурсам, содержащим информацию, запрещённую к распространению среди детей, ограниченную к распространению среди детей определённых возрастных категорий, а также не соответствующую задачам образования (Приложение 1);
- использовать сети связи общего пользования для осуществления экстремистской деятельности;
- осуществлять любые сделки через сеть «Интернет»;
- осуществлять загрузку файлов на компьютеры Школы без разрешения контролирующего работника.

9.6. При обнаружении ресурса, содержащего негативную информацию, обучающийся обязан незамедлительно сообщить об этом контролирующему работнику.

## 10. Порядок действий при обнаружении негативной информации

10.1. Контролирующий работник, получивший сообщение обучающегося о выявлении ресурса с негативной информацией либо самостоятельно выявивший такой ресурс, обязан зафиксировать доменный адрес ресурса и время его обнаружения и сообщить об этом Ответственному.

10.2. Ответственный обязан:

- принять информацию от работника;
- направить информацию о выявлении ресурса оператору Реестра безопасных образовательных сайтов в течение суток;
- в случае явного нарушения обнаруженным ресурсом законодательства Российской Федерации сообщить о нём по специальной «горячей линии» (Роскомнадзор) для принятия мер в соответствии с законодательством Российской Федерации.

10.3. Передаваемая информация должна содержать: доменный адрес ресурса; сообщение о тематике ресурса; дату и время обнаружения; информацию об установленных в Школе технических средствах ограничения доступа к информации.

10.4. В случае отказа (блокирования) доступа к ресурсу, разрешённому в Школе, работник также сообщает об этом Ответственному.

## 11. Просветительская работа в области информационной безопасности

11.1. В Школе организуется преподавание обучающимся основ информационной безопасности в рамках реализации образовательной программы в течение учебного года.

11.2. Проводятся Единый урок безопасности в сети «Интернет» (октябрь) и мероприятия проекта «Сетевичок» (октябрь–ноябрь).

11.3. Осуществляется информирование родителей (законных представителей) обучающихся о существующих угрозах в сети «Интернет», методах и способах защиты детей от негативной информации, а также об ответственности за нарушение требований законодательства.

11.4. Оформляется и обновляется стенд «Информационная безопасность», на официальном сайте Школы размещается информация по вопросам обеспечения информационной безопасности детей.

## 12. Ответственность за нарушение Положения

12.1. За неисполнение или нарушение Положения к работникам Школы могут быть применены меры дисциплинарного взыскания в соответствии с Федеральным законом № 273-ФЗ; к обучающимся — меры дисциплинарного воздействия, предусмотренные Уставом Школы и локальными нормативными актами, возможна постановка на внутришкольный контроль.

## 13. Заключительные положения

13.1. Положение вступает в силу со дня его утверждения приказом директора Школы.

13.2. Положение размещается на официальном сайте Школы в сети «Интернет».

13.3. При актуализации Методических рекомендаций, утверждённых письмом Минпросвещения России от 07.06.2019 № 04-474, Школа приводит Положение в соответствие с новой редакцией.

13.4. Изменения и дополнения в Положение вносятся в том же порядке, что и его принятие.

Приложение № 1
к Положению об ограничении доступа обучающихся к видам информации,
распространяемой посредством сети «Интернет», причиняющей вред здоровью
и (или) развитию детей, а также не соответствующей
задачам образования ГБОУ СОШ с. Герасимовка

**ПЕРЕЧЕНЬ видов информации, запрещённой к распространению посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования**

**I. Информация, запрещённая к распространению среди детей согласно части 2 статьи 5 Федерального закона от 29.12.2010 № 436-ФЗ (в действующей редакции):**

| № | Вид информации | Характеристика |
|---|---|---|
| 1 | Побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий | Сайты, сетевые СМИ, социальные сети, приложения, содержащие описания и (или) изображения способов причинения вреда своему здоровью, самоубийства; обсуждения таких способов и их последствий, мотивирующие на совершение таких действий |
| 2 | Способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия и никотинсодержащую продукцию, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством | Реклама, объявления, предложения, направленные на продажу детям наркотических средств, психотропных и одурманивающих веществ, табачных изделий, алкогольной продукции, а также вовлечение в азартные игры, проституцию, бродяжничество, попрошайничество |
| 3 | Обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным | Материалы, содержащие акты насилия или жестокости, обосновывающие, оправдывающие и вовлекающие детей в такие акты, формирующие культуру насилия и жестокости |
| 4 | Содержащая изображение или описание сексуального насилия | Материалы, содержащие изображение или описание сексуального насилия (тексты, фотографии, рисунки, аудио- и видеоматериалы) |
| 5 | Пропагандирующая нетрадиционные сексуальные отношения и (или) предпочтения, смену пола | Материалы, рекламирующие и изображающие нетрадиционные сексуальные отношения и (или) предпочтения, пропагандирующие смену пола |
| 6 | Оправдывающая противоправное поведение | Материалы, содержащие призывы и вовлечение детей в противоправное поведение и одобряющие его |
| 7 | Содержащая нецензурную брань | Материалы, содержащие нецензурную брань |
| 8 | Содержащая информацию порнографического характера | Материалы, содержащие текстовые описания, фотографии, рисунки, аудио- и видеоматериалы порнографического характера |
| 9 | О несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения, | Материалы, содержащие перечисленные сведения о пострадавшем несовершеннолетнем |

| | | |
|---|---|---|
| | аудиозапись голоса, место жительства или временного пребывания, место учёбы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего | |

**II. Информация, распространение которой среди детей определённых возрастных категорий ограничено согласно части 3 статьи 5 Федерального закона № 436-ФЗ (в действующей редакции):**

| № | Вид информации | Характеристика |
|---|---|---|
| 10 | Представляемая в виде изображения или описания жестокости, физического и (или) психического насилия (за исключением сексуального насилия), преступления или иного антиобщественного действия | Материалы, содержащие текстовые описания, фотографии, рисунки, видеоматериалы по данной теме |
| 11 | Вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий | Материалы, содержащие текстовые описания, фотографии, рисунки, видеоматериалы по данной теме |
| 12 | Представляемая в виде изображения или описания половых отношений между мужчиной и женщиной | Материалы, содержащие текстовые описания, фотографии, рисунки, видеоматериалы по данной теме |
| 13 | Содержащая бранные слова и выражения, не относящиеся к нецензурной брани | Материалы, содержащие бранные слова и выражения, не относящиеся к нецензурной брани |

**III. Информация, не соответствующая задачам образования (перечень приведён для целей настоящего Положения на основании Методических рекомендаций, утверждённых письмом Минпросвещения России от 07.06.2019 № 04-474; нормативного закрепления в Федеральном законе № 436-ФЗ не имеет):**

| № | Вид информации | Характеристика |
|---|---|---|
| 14 | Компьютерные и сетевые игры, за исключением соответствующих задачам образования | Порталы браузерных игр, массовые многопользовательские игры и другие игры, игровой процесс которых осуществляется через сеть «Интернет» |
| 15 | Ресурсы, базирующиеся либо ориентированные на обеспечение анонимности распространителей и потребителей информации | Анонимные форумы, чаты, доски объявлений и гостевые книги, анонимайзеры и другие программы и сервисы |
| 16 | Банки рефератов, эссе, дипломных работ, готовых домашних заданий и других ресурсов, предоставляющих готовые решения | Сайты готовых рефератов, эссе, курсовых и дипломных работ, готовых домашних заданий, решебников, ответов на контрольные и самостоятельные работы |
| 17 | Онлайн-казино и тотализаторы | Информация об электронных казино, тотализаторах и других видах игр на денежные средства или их аналоги, способах доступа к ним |
| 18 | Мошеннические сайты | Сайты, навязывающие услуги на базе СМС-платежей, сайты, обманным путём собирающие |

| | | |
|---|---|---|
| | | личную информацию (фишинг) |
| 19 | Магия, колдовство, чародейство, ясновидящие, приворот по фото, теургия, волшебство, некромания и секты | Материалы, оказывающие психологическое воздействие на детей через обращение к тайным силам |
| 20 | Ресурсы, содержащие рекламу и направленные на продажу товаров и (или) услуг детям | Материалы, побуждающие несовершеннолетних приобретать товары и (или) услуги |
| 21 | Службы знакомств, социальные сети, мессенджеры и сервисы для организации сетевого общения (за исключением образовательных ресурсов) | Сервисы, направленные на организацию общения между пользователями |
| 22 | Ресурсы, нарушающие исключительные права (авторские права) | Торренты, пиринговые сети и другие ресурсы, предоставляющие контент и программное обеспечение с нарушением авторских прав |
| 23 | Пропаганда национализма, фашизма и межнациональной розни | Материалы, содержащие соответствующие описания, изображения и видеоматериалы |
| 24 | Ресурсы, ориентированные на предоставление неправдивой информации об истории России и формирование неуважительного отношения к ней | Материалы, содержащие неправдивую информацию об истории России |
| 25 | Ресурсы, ориентированные на продажу документов об образовании и (или) обучения без прохождения обучения | Сайты, предлагающие покупку документов об образовании |

Приложение № 2
к Положению об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования ГБОУ СОШ с. Герасимовка

**План мероприятий по обеспечению информационной безопасности обучающихся на 20___/20___ учебный год**

| № | Мероприятие | Сроки |
|---|---|---|
| 1 | Изучение нормативно-правовой базы (включая письмо Минпросвещения России от 07.06.2019 № 04-474, письмо от 24.08.2021 № 04-ПГ-МП-30120, приказ Минцифры России от 01.12.2020 № 644), методических рекомендаций; издание (актуализация) организационно-распорядительных документов | Июнь–август |
| 2 | Проверка подключения к ЕСПД и исполнения услуг связи (контентная фильтрация) по действующим государственным контрактам; взаимодействие с ПАО «Ростелеком» | Июнь–август |
| 3 | Настройка АРМ и сетевого оборудования в соответствии с требованиями к подключению к ЕСПД; установка, конфигурация и настройка режимов работы средств контентной фильтрации | Июнь–август |
| 4 | Организация трёх раздельных сетей Wi-Fi (обучающиеся, работники, гостевая) и порядка идентификации пользователей; издание приказа о порядке использования личных устройств обучающихся | Август |
| 5 | Ознакомление работников с Методическими рекомендациями и локальными нормативными актами по вопросам информационной безопасности обучающихся | Август |
| 6 | Тестирование СКФ по единым правилам; проверка безопасного поиска, статистики обращений и актуальности правил фильтрации | Август–сентябрь |

| | | |
|---|---|---|
| 7 | Информирование работников, обучающихся и родителей об ответственности за нарушение требований законодательства и локальных актов по вопросам информационной безопасности | Август–сентябрь |
| 8 | Информирование родителей об угрозах в сети «Интернет», методах и способах защиты детей от негативной информации | Сентябрь–октябрь |
| 9 | Ознакомление работников с Реестром безопасных образовательных сайтов (РБОС) | Август |
| 10 | Проведение периодического контроля состояния системы обеспечения информационной безопасности: проверка журнала СКФ, журнала учёта подключений к Wi-Fi, заявок в личном кабинете ЕСПД | Не менее 3 раз в течение учебного года |
| 11 | Организация преподавания обучающимся основ информационной безопасности в рамках реализации образовательной программы | В течение учебного года |
| 12 | Проведение Единого урока по безопасности в сети «Интернет» | Октябрь |
| 13 | Проведение серии мероприятий проекта «Сетевичок» для обучающихся | Октябрь–ноябрь |
| 14 | Оформление и обновление стенда «Информационная безопасность»; размещение информации на официальном сайте Школы | В течение учебного года |
| 15 | Прохождение педагогическими и иными работниками повышения квалификации по направлению «Безопасное использование сайтов в сети «Интернет» в образовательном процессе» | Раз в два календарных года |
| 16 | Ведение (актуализация) локальных нормативных актов в области информационной безопасности обучающихся при необходимости | В течение учебного года |

Приложение № 3
к Положению об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования ГБОУ СОШ с. Герасимовка

**АКТ проверки эффективности использования системы контентной фильтрации (СКФ)**

Государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа с. Герасимовка муниципального района Алексеевский Самарской области

**АКТ № ___**

проверки эффективности использования системы контентной фильтрации (СКФ)

с. Герасимовка «___» _____ 20___ г.

Комиссия в составе: председатель — заместитель директора _____ (Ф.И.О.); члены комиссии: ответственный за организацию работы с сетью «Интернет» и ограничение доступа _____ (Ф.И.О.); член Совета по обеспечению информационной безопасности обучающихся _____ (Ф.И.О.), назначенная приказом директора Школы от «___» _____ 20___ г. № ___, провела проверку эффективности использования системы контентной фильтрации в ГБОУ СОШ с. Герасимовка за период с «___» _____ 20___ г. по «___» _____ 20___ г.

**По результатам проверки установлено:**

| **№** | **Проверяемый вопрос** | **Результат (соответствует / не соответствует)** | **Примечание** |
|---|---|---|---|
| 1 | Подключение Школы к ЕСПД; работоспособность СКФ на всех АРМ и в сетях Wi-Fi | _____ | _____ |
| 2 | Блокирование доступа к ресурсам, включённым в Единый реестр, и к ресурсам с информацией из Приложения № 1 к | _____ | _____ |

| | | | |
|---|---|---|---|
| | Положению (тестовые обращения, отображение страницы блокировки) | | |
| 3 | Принудительное включение безопасного поиска в используемых поисковых системах | _____ | _____ |
| 4 | Ведение и доступность статистики обращений к ресурсам сети «Интернет», в том числе заблокированных | _____ | _____ |
| 5 | Актуализация правил фильтрации с учётом РБОС (не позднее 3 рабочих дней после изменения перечня) | _____ | _____ |
| 6 | Отсутствие отключений СКФ на АРМ, используемых обучающимися | _____ | _____ |
| 7 | Ведение журнала работы СКФ (Приложение № 4 к Положению), полнота фиксации событий | _____ | _____ |
| 8 | Функционирование идентификации пользователей при подключении через сети Wi-Fi | _____ | _____ |
| 9 | Отсутствие несанкционированных точек доступа Wi-Fi | _____ | _____ |
| 10 | Отсутствие обращений обучающихся к негативной информации по данным статистики СКФ за отчётный период (либо принятые меры по выявленным случаям) | _____ | _____ |

**Выводы комиссии:**

1. СКФ, реализуемая на базе ЕСПД (ПАО «Ростелеком»), соответствует требованиям Методических рекомендаций (письмо Минпросвещения России от 07.06.2019 № 04-474) и приказу Минкомсвязи России от 16.06.2014 № 161: да / нет (ненужное зачеркнуть).
2. Выявленные недостатки:

_____.

3. Принятые меры (заявки в личный кабинет ЕСПД, обращения в техническую поддержку ПАО «Ростелеком», иное):

_____.

Акт направлен директору Школы «___» _____ 20___ г.; доклад рассмотрен на Педагогическом совете Школы (протокол от «___» _____ 20___ г. № ___).

Председатель комиссии: _____ / _____ /

Члены комиссии: _____ / _____ /

_____ / _____ /

Приложение № 4
к Положению об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования ГБОУ СОШ с. Герасимовка

**ЖУРНАЛ работы системы контентной фильтрации (СКФ)**

**Правила ведения журнала:**

1. Журнал ведёт ответственный за организацию работы с сетью «Интернет» и ограничение доступа, назначенный приказом директора Школы.
2. В журнал вносятся сведения о: блокировании ресурсов с негативной информацией (при фиксации работником или обучающимся); заявках на блокирование и разблокирование ресурсов, направленных в личный кабинет ЕСПД и техническую поддержку ПАО «Ростелеком»; сбоях работы СКФ; случаях

отключения СКФ (на основании письменного согласия директора Школы); фактах обнаружения несанкционированных точек доступа Wi-Fi.

3. Записи вносятся в день события, без пропуска строк; исправления заверяются подписью Ответственного.

4. Журнал хранится у Ответственного и предъявляется по требованию директора Школы и органов управления образованием.

Начат: «___» _____ 20___ г. Окончен: «___» _____ 20___ г.

| **№ записи** | **Дата, время** | **Доменный адрес (URL) ресурса** | **Характер события (блокирование / разблокирование / сбой / заявка / отключение СКФ)** | **Принятые меры** | **Отметка о передаче информации (ЛК ЕСПД, РБОС, «горячая линия»)** |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Приложение № 5
к Положению об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования ГБОУ СОШ с. Герасимовка

**ИНСТРУКЦИЯ для обучающихся по обеспечению информационной безопасности при использовании сети «Интернет»**

(размещается в учебных кабинетах, в которых осуществляется доступ в сеть «Интернет»)

1. Работай в сети «Интернет» только в учебных целях и только с разрешения учителя.
2. Не переходи по ссылкам от незнакомых людей и не открывай всплывающие окна с сомнительным содержанием.
3. Если на экране появилась информация, которая вызывает тревогу, страх или стеснение (жестокость, сцены насилия, неприличные изображения, призывы к опасным действиям), — прекрати просмотр и сразу сообщи учителю. Не закрывай страницу до прихода учителя: по адресу страницы будет направлена заявка на блокирование.
4. Не сообщай в сети «Интернет» свои личные данные (фамилию, адрес, номер телефона, название школы) и данные своих родных; не выкладывай фотографии без разрешения родителей.
5. Не скачивай файлы и программы на компьютеры Школы без разрешения работника Школы.
6. Не используй анонимайзеры и программы для обхода блокировок; не раздавай Wi-Fi со своего устройства — это запрещено Положением Школы.
7. Если тебя обижают или угрожают тебе в сети «Интернет», не отвечай агрессией: сохрани переписку (скриншоты) и сообщи взрослому, которому доверяешь.
8. Помни: информация в сети «Интернет» не всегда правдива. Проверяй источники и пользуйся ресурсами, рекомендованными учителем (Реестр безопасных образовательных сайтов).
9. Соблюдай вежливость в общении в сети «Интернет» так же, как и в жизни.

**Куда обратиться за помощью:**

— Детский телефон доверия (круглосуточно, бесплатно, анонимно): 8-800-2000-122;

— горячая линия Роскомнадзора для сообщений о запрещённой информации: https://rkn.gov.ru/treatments/ask-question/ .

Приложение № 6
к Положению об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования ГБОУ СОШ с. Герасимовка

**Пункты для внесения в должностные инструкции педагогических работников ГБОУ СОШ с. Герасимовка**

(рекомендуется включить в раздел «Обязанности» должностных инструкций педагогических работников):

1. Знать Положение об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, Правила использования сети «Интернет» на учебный год и инструкцию для обучающихся по обеспечению информационной безопасности (Приложение № 5 к Положению).
2. Осуществлять контроль использования обучающимися сети «Интернет» во время проводимых занятий в порядке, установленном разделом 8 Положения.
3. Организовывать работу обучающихся в сети «Интернет» только с ресурсами, соответствующими целям образовательного процесса; не оставлять обучающихся без присмотра при работе с АРМ, имеющими доступ к сети «Интернет».
4. Принимать меры по пресечению обращений обучающихся к ресурсам, содержащим негативную информацию (перечень — в Приложении № 1 к Положению).
5. При обнаружении ресурса с негативной информацией фиксировать его доменный адрес и время обнаружения и незамедлительно сообщать ответственному за организацию работы с сетью «Интернет» и ограничение доступа.
6. Информировать классного руководителя о преднамеренных попытках обучающихся обратиться к ресурсам с негативной информацией.
7. Сообщать ответственному о блокировании ресурсов, необходимых для образовательного процесса, для принятия решения о разблокировании в порядке, установленном Положением.
8. Не отключать систему контентной фильтрации без письменного согласия директора (заместителя директора) Школы.
9. Знакомить обучающихся с инструкцией по обеспечению информационной безопасности при использовании сети «Интернет» в начале учебного года и далее не реже одного раза в учебную четверть.
10. Проводить разъяснительную работу с обучающимися и родителями (законными представителями) по вопросам информационной безопасности.
11. Участвовать в мероприятиях по обеспечению информационной безопасности обучающихся согласно плану мероприятий (Приложение № 2 к Положению).