

СОГЛАСОВАНО
Педагогическим советом
МБОУ «СОШ № 31»
Протокол от 30.08.2023г.

УТВЕРЖДЕНО
приказом директора
МБОУ «СОШ № 31»
От 30.08.2023г. № 75/01-09

Положение об обеспечении информационной безопасности

1. Общие положения

- 1.1. Настоящее Положение об обеспечении информационной безопасности в МБОУ «Средняя общеобразовательная школа №31» г. Калуги (далее – Положение) определяет систему правовых, организационных и технических мероприятий, направленных на обеспечение информационной безопасности обучающихся и работников в МБОУ «Средняя общеобразовательная школа №31» г. Калуги.
- 1.2. Положение разработано в соответствии с:
- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
 - Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
 - Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
 - Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
 - Федеральным законом от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»;
 - Доктриной информационной безопасности Российской Федерации, утв. Указом Президента РФ от 05.12.2016 № 646;
 - Концепцией информационной безопасности детей, утв. Распоряжением Правительства РФ от 02.12.2015 № 2471-р;
 - Порядком организации и осуществления образовательной деятельности по основным общеобразовательным программам – образовательным программам начального общего, основного общего и среднего общего образования, утвержденным приказом Минобрнауки от 30.08.2013 № 1015;
 - Порядком организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам, утв. Приказом Минпросвещения России от 09.11.2018 № 196;
 - Порядком применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ, утв. приказом Минобрнауки от 23.08.2017 № 816;
 - 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»;
- ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения, утв. и введен в действие Приказом Ростехрегулирования от 18.12.2008 № 532-ст;
 - ГОСТ Р 526532006. Национальный стандарт Российской Федерации. Информационно-коммуникационные технологии в образовании. Термины и определения, утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 419-ст;
 - ГОСТ Р 53620-2009. Национальный стандарт Российской Федерации. Информационно-коммуникационные технологии в образовании. Электронные образовательные ресурсы. Общие положения, утв. и введен в действие Приказом Ростехрегулирования от 15.12.2009 № 956-ст;
 - Методическими материалами для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет, направленными Письмом Минобрнауки России от 28.04.2014 № ДЛ-115/03;
 - Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети Интернет, направленными Письмом Минобрнауки России от 14.05.2018 № 08-1184;
 - Уставом МБОУ «Средняя общеобразовательная школа №31» г. Калуги
- 1.3. В Положении используются следующие термины и определения:
- 1.3.1. **информационная безопасность детей** - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию;
 - 1.3.2. **доступ детей к информации** - возможность получения и использования детьми свободно распространяемой информации;
 - 1.3.3. **знак информационной продукции** - графическое и (или) текстовое обозначение информационной продукции в соответствии с классификацией информационной продукции, предусмотренной частью 3 статьи 6 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»;
 - 1.3.4. **места, доступные для детей** - общественные места, доступ ребенка в которые и (или) нахождение ребенка в которых не запрещены, в том числе общественные места, в которых ребенок имеет доступ к продукции средств массовой информации и (или) размещаемой в информационно-телекоммуникационных сетях информационной продукции;
 - 1.3.5. **информационная продукция** - предназначенные для оборота на территории Российской Федерации продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, программы для электронных вычислительных машин (программы для ЭВМ) и базы данных, а также информация, распространяемая посредством зрелищных мероприятий, посредством информационно- телекоммуникационных сетей, в том числе сети Интернет, и сетей подвижной радиотелефонной связи;
 - 1.3.6. **информационная продукция для детей** - информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей;
 - 1.3.7. **информация, причиняющая вред здоровью и (или) развитию детей** - информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с настоящим Федеральным законом;
 - 1.3.8. **персональные данные** – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

- 1.3.9. **оператор персональных данных (оператор)** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- 1.3.10. **обработка персональных данных** – действие (операция) или совокупность действий (операций) с персональными данными с использованием и без использования средств автоматизации, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;
- 1.4. Система информационной безопасности является неотъемлемой частью системы комплексной безопасности МБОУ «Средняя общеобразовательная школа №31» г. Калуги (далее - Школа).
- 1.5. Функционирование системы информационной безопасности в Школе обеспечивается применением комплекса правовых, организационных и технических мер защиты, в результате чего снижается или исключается риск, связанный с причинением информационной продукцией, используемой в образовательной деятельности, вреда здоровью и (или) физическому, психическому, духовному, нравственному развитию несовершеннолетних обучающихся.
- 1.6. Использование сети Интернет в образовательной деятельности допускается только при условии применения административных и организационных мер, технических (программных, программно-аппаратных) средств защиты обучающихся от информации, не совместимой с задачами образования и воспитания, иной информации, распространение которой в Российской Федерации запрещено, информации, причиняющей вред здоровью и (или) развитию детей.

2. Основные цели и задачи функционирования системы информационной безопасности

- 2.1. Система информационной безопасности направлена на защиту единого информационного образовательного пространства Школы от незаконного проникновения, на предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в локальных сетях, а также недопущения доступа обучающихся и работников учреждения к информации, которая запрещена или ограничена к распространению в Российской Федерации.
- 2.2. Система информационной безопасности Школы направлена на решение следующих задач:
- 2.2.1. защита прав и законных интересов обучающихся в образовательной деятельности, защита обучающихся от информации, причиняющей вред их здоровью и (или) развитию и (или) не соответствующей задачам образования;
- 2.2.2. разграничение объемов и содержания информации, которая может быть доступна различным категориям пользователей;
- 2.2.3. предотвращение утечки, хищения, утраты, подделки информации Школы;
- 2.2.4. предотвращение несанкционированных действий по уничтожению модификации, искажению, копированию, блокированию информации учреждения;
- 2.2.5. предотвращение других форм незаконного вмешательства в информационные ресурсы учреждения и его локальную сеть.

3. Организационно-административные меры, направленные на защиту детей от информации, причиняющей вред их здоровью и (или) развитию.

- 3.1. Приказом директора в Школе назначается лицо, ответственное за обеспечение информационной безопасности. В обязанности ответственного за обеспечение информационной безопасности в том числе входит:
- 3.1.1. контроль функционирования системы контентной фильтрации;
 - 3.1.1. контроль функционирования антивирусной защиты, поддержание в актуальном состоянии антивирусных баз автоматической проверке ПК, локальной сети и внешних носителей на наличие вирусов;
 - 3.1.2. контроль соблюдения требований по обеспечению информационной безопасности при проведении технического обслуживания и ремонтных работ персональных компьютеров;
 - 3.1.3. оценка рисков информационной безопасности учреждения;
 - 3.1.4. выявление угроз безопасности оборудованию и локальной сети Школы;
 - 3.1.5. проведение инструктажа работников Школы по правилам работы с используемыми аппаратно-программными средствами и осуществление контроля за действиями пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования,
 - 3.1.6. информирование обучающихся, родителей несовершеннолетних обучающихся, работников Школы о порядке использования сети Интернет и контроль за использованием сети Интернет обучающимися и работниками.
- 3.2. В Школе разрабатываются и утверждаются локальные нормативные акты, регламентирующие:
- 3.2.1. политику обработки персональных данных, права и обязанности обучающихся и работников Школы в сфере защиты персональных данных;
 - 3.2.2. порядок доступа и использования сети Интернет в Школе;
 - 3.2.3. организацию контроля использования сети Интернет в Школе;
 - 3.2.4. организацию контроля за библиотечным фондом и предотвращение доступа обучающихся к информации экстремистского характера, к информации, запрещенной для распространения среди детей и (или) не соответствующей возрасту обучающихся.
- 3.3. В Школе оказывается организационная и методическая поддержка работникам в области безопасной работы с информационными ресурсами, информационными образовательными технологиями, в том числе, путем их направления на повышение квалификации по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети Интернет.
- 3.4. В Школе на регулярной основе осуществляется информирование работников, обучающихся и их родителей (законных представителей) об ответственности за нарушение требований законодательства Российской Федерации, локальных нормативных и организационно-распорядительных актов Школы по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети «Интернет».
- 3.5. В Школе разрабатывается, реализуется *и совершенствуется* комплекс мероприятий, направленный на правовое просвещение обучающихся и родителей (законных представителей) несовершеннолетних обучающихся в сфере информационной безопасности, на формирование навыков обучающихся безопасной работы в информационно-телекоммуникационных сетях.
- 3.6. Жалобы или претензии о нарушениях законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, включая несоответствие

применяемых административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, установленным законодательством требованиями, 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 рассматриваются руководством Школы в срок, не превышающий 7 (семи) рабочих дней со дня получения.

- 3.7. В случае получения обращений, жалоб или претензий о наличии доступа детей к информации, запрещенной для распространения среди детей, установление причин и условий возникновения такого доступа и принятие мер по их устранению осуществляется руководством Школы незамедлительно.
- 3.8. Мониторинг осуществления организационно- административных мер, направленных на защиту детей от информации, причиняющей вред их здоровью и (или) развитию осуществляется заместителем директора в рамках своих полномочий.

4. Информация, используемая в образовательной деятельности и контроль за ее содержанием.

- 4.1. Информация и (или) информационная продукция, используемая в образовательной деятельности, осуществляемой в учреждении, должна соответствовать требованиям законодательства Российской Федерации к защите детей от информации, причиняющей вред их здоровью и (или) развитию, соответствовать содержанию и задачам образования.
- 4.2. При осуществлении образовательной деятельности в Школе обеспечивается доступ обучающихся и работников к:
 - 4.2.1. печатной продукции, которая входит в библиотечный фонд Школы;
 - 4.2.2. электронным образовательным ресурсам, прошедшим педагогическую экспертизу, рекомендованным и (или) сформированным органами государственной власти, осуществляющими управление в сфере образования, подведомственными им организациями; разработанными издательствами, выпускающими учебную литературу, учреждениями высшего и среднего образования, российскими библиотеками и иными уполномоченными или допущенными органами и организациями;
 - 4.2.3. общедоступным государственным и региональным информационным системам;
 - 4.2.4. информационно-телекоммуникационной сети Интернет в порядке, установленном локальным нормативным актом Школы.
- 4.3. В работе и (или) общении с обучающимися педагогическим работникам или иным работникам Школы не допускается использовать информацию:
 - 4.3.1. которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иную информацию, за распространение которой предусмотрена уголовная или административная ответственность;
 - 4.3.2. запрещенную для распространения среди детей в соответствии со ст.5 Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
 - 4.3.3. имеющую знак информационной продукции, не соответствующий возрасту обучающегося (обучающихся);
 - 4.3.4. полученную с нарушением авторских или смежных прав;
 - 4.3.5. имеющую конфиденциальный характер в соответствии с действующим законодательством и (или) локальными нормативными актами Школы.
- 4.4. Мониторинг содержания информационной продукции, используемой в образовательной деятельности педагогических работников осуществляется предметными кафедрами, а также администрацией в рамках внутришкольного контроля.
- 4.5. В образовательной и (или) досуговой деятельности с обучающимися, организуемой и проводимой работниками Школы, не допускается посещения зрелищных или иных мероприятий, билеты на которые (афиши или иная информация о мероприятии) содержат знак информационной продукции, не соответствующий возрасту обучающегося (обучающихся).
- 4.6. В Школе осуществляется административный контроль за соблюдением возрастной классификации информационной продукции, приобретаемой и (или) используемой в

образовательной и (или) досуговой деятельности.

- 4.7. В процессе осуществления образовательной деятельности с использованием информационно-компьютерных технологий педагогическими работниками осуществляется контроль за использованием обучающимися сети Интернет, в том числе, визуальный контроль.
- 4.8. При обнаружении угроз информационной безопасности Школы, несанкционированного доступа к локальной сети, а также обнаружении доступа к ресурсу, содержание которого может нанести вред здоровью и (или) развитию обучающихся, работники Школы обязаны незамедлительно сообщить об этом руководству для принятия соответствующих мер.
- 4.9. Работник, ответственный за обеспечение информационной безопасности, при получении информации, указанной в п. 4.8. настоящего Положения незамедлительно:
 - 4.9.1. устанавливает обстоятельства получения доступа к ресурсу сети Интернет, содержащему информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей;
 - 4.9.2. идентифицирует ресурс сети Интернет;
 - 4.9.3. в течение 1 (одного) рабочего дня с момента получения информации, указанной в п.4.8. настоящего Положения, проводит мероприятия, направленные на ограничение доступа к ресурсу сети Интернет, содержащему информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей (вносит изменения в политики доступа, применяемые в технических средствах контентной фильтрации, вносит изменения в конфигурацию технических средств контентной фильтрации, в случае необходимости предпринимает другие меры).
 - 4.9.4. проводит анализ обстоятельств, послуживших причиной доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей.
 - 4.9.5. вносит директору Школы на основе проведенного анализа предложения по совершенствованию системы контентной фильтрации в целях минимизации количества инцидентов, связанных с получением доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей.
- 4.10. В порядке реагирования на инцидент, угрожающий информационной безопасности Школы и (или) обучающихся и работников Школы, руководством может быть направлено соответствующее сообщение о наличии на страницах сайтов в сети Интернет информации, распространение которой в Российской Федерации запрещено в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также в органы внутренних дел.

5. Организационно-технические мероприятия по формированию безопасных условий доступа обучающихся к ресурсам сети Интернет

- 5.1. К техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, применяемым при предоставлении доступа к информации, распространяемой посредством сети Интернет, относятся:
 - 5.1.1. средства ограничения доступа к техническим средствам доступа к сети Интернет;

- 5.1.2. средства ограничения доступа к сети Интернет с технических средств третьих лиц;
- 5.1.3. средства ограничения доступа к запрещенной для распространения среди детей информации, размещенной на сайтах в сети Интернет.
- 5.2. В Школе обеспечивается антивирусная защита компьютерной техники, систематически проводится обновление антивирусных программ.
- 5.3. Для приобретения и использования программного обеспечения в образовательной и иной деятельности Школы проводится проверка его подлинности.
- 5.4. В Учреждении с установленной периодичностью осуществляется контроль:
 - 5.4.1. эксплуатации технических средств контентной фильтрации – постоянно;
 - 5.4.2. функционирования технических средств контентной фильтрации и их конфигурации – не реже 2 раз в год;
 - 5.4.3. организации доступа к сети Интернет в целях исключения возможности несанкционированного использования сети Интернет в Школе – постоянно;
 - 5.4.4. функционирования технических средств, применяемых при организации доступа к сети Интернет, и их конфигурации (компьютерное оборудование, сетевое оборудование, системное и прикладное программное обеспечение) – не реже 2 раз в год;
 - 5.4.5. изменения конфигурации технических средств, применяемых при организации доступа к сети Интернет, контроль наличия в их составе аппаратных, программных средств, предназначенных для нарушения функционирования технических средств контентной фильтрации – не реже 2 раз в год;
 - 5.4.6. ведения журналов регистрации посещений ресурсов сети Интернет – не реже 1 раза в месяц;
 - 5.4.7. функционирования системы антивирусной защиты – не реже 1 раза в месяц;
 - 5.4.8. наличия доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, путем осуществления попыток получения доступа к таким ресурсам сети Интернет – не реже 1 раза в квартал;
- 5.5. В учреждении не допускается обучающимися и работниками, а также иными лицами самовольная установка программного обеспечения на компьютерную технику Школы, либо использование не принадлежащих Школе программ и оборудования.
- 5.6. Мониторинг осуществления организационно-технических мер, направленных на обеспечение информационной безопасности учреждения осуществляется заместителем директора Школы по ресурсам в рамках своих полномочий.

6. Обучение и просвещение в сфере информационной безопасности

- 6.1. В рамках образовательной деятельности в Школе осуществляется обучение безопасным способам работы в информационно-телекоммуникационных сетях, в план воспитательной работы Школы включаются мероприятия, направленные на повышение медиаграмотности обучающихся, формированию навыков безопасного поведения в сети Интернет.

- 6.2. В Школе проводятся образовательные и консультационные мероприятия с родителями обучающихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в сеть Интернет.
- 6.3. На информационных стендах, расположенных в Школе и в кабинетах, оснащенных персональными устройствами для выхода в сеть Интернет, размещаются информационные памятки, содержащие основные советы по обеспечению информационной безопасности учащихся.
- 6.4. На официальном сайте Школы размещается специализированный раздел «Безопасность», в рамках которого предусмотрено размещение локальных нормативных актов в сфере обеспечения информационной безопасности обучающихся, нормативно-правовых документов, регламентирующих обеспечение информационной безопасности несовершеннолетних, методические рекомендации, информационные памятки для работников, обучающихся и их родителей, направленные на повышение информационной грамотности и обеспечение информационной безопасности детей.

7. Заключительные положения

- 7.1. Положение вступает в силу с момента его утверждения приказом директора Школы.
- 7.2. Положение отменяется или изменяется в случае изменения действующего законодательства, а также при наличии иных нормативно-правовых оснований, влекущих изменение, дополнение или отмену закрепленных в нем положений.
- 7.3. Положение размещается на информационных стендах Школы и на официальном сайте Школы в сети Интернет.

