«Утверждаю»

Директор «ИП Будаева О.Е.»

_____ О.Е. Будаева

Положение об обеспечении информационной безопасности

1. Общие положения

1. Настоящие положения об обеспечении информационной безопасности определяют систему организационных, правовых, технических мероприятий направленные на обеспечение информационной безопасности воспитанников и работников д/с «Журавленок» ИП «Будаева О.Е.».

2. Положение разработано в соответствии:

- Федеральным законом от 29.11.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– Федеральным законом от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

– Федеральным законом от 27.06.2006 № 152-ФЗ «О персональных данных»;

– Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причин и вред их здоровью и развитию»;

– Федеральным законом от 25.07.2002 № 114-ФЗ «О противодействии экстремисткой деятельности»;

– Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646.

– Концепцией информационной безопасности детей, утвержденной Распоряжением Правительства Российской Федерации от 02.12.2015 № 2471-р.

– Порядком применения организации, осуществляющими 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;

1.1. В Положении используются следующие термины и определения:

информационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию;

доступ детей к информации - возможность получения и использования детьми свободно распространяемой информации;

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»;

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;

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;

информационная продукция для детей - информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей;

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;

персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

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;

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;

1.2. Система информационной безопасности является неотъемлемой частью системы комплексной безопасности организации (д/с «Журавленок» ИП «Будаева О.Е.»).

1.3. 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.

1.4. 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

1.5. Система информационной безопасности направлена защиту единого информационного образовательного пространства организации 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.

1.6. Система информационной безопасности Школы направлена на решение следующих задач:

1.6.1. 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;

1.6.2. разграничение объемов и содержания информации, которая может быть доступна различным категориям пользователей;

1.6.3. предотвращение утечки, хищения, утраты, подделки информации организации;

1.6.4. предотвращение несанкционированных действий по уничтожению модификации, искажению, копированию, блокированию информации организации;

1.6.5. предотвращение других форм незаконного вмешательства в информационные ресурсы организации 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 организации 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;

3.1.2. контроль функционирования антивирусной защиты, поддержание в актуальном состоянии антивирусных баз автоматической проверке ПК, локальной сети и внешних носителей на наличие вирусов;

3.1.3. контроль соблюдения требований по обеспечению информационной безопасности при проведении технического обслуживания и ремонтных работ персональных компьютеров;

3.1.4. оценка рисков информационной безопасности организации;

3.1.5. выявление угроз безопасности оборудованию и локальной сети организации;

3.1.6. проведение инструктажа работников организации 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,

3.1.7. информирование воспитанников, родителей воспитанников, работников организации о порядке использования сети Интернет.

3.2. В организации разрабатываются и утверждаются локальные нормативные акты, регламентирующие:

3.2.1. политику обработки персональных данных, права и обязанности воспитанников и работников в сфере защиты персональных данных;

3.2.2. порядок доступа и использования сети Интернет в организации;

3.2.3. организацию контроля использования сети Интернет в организации;

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 организации 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 организации на регулярной основе осуществляется информирование работников, воспитанников и их родителей (законных представителей) об ответственности за нарушение требований законодательства Российской Федерации, локальных нормативных и организационно- распорядительных актов организации по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети «Интернет».

3.5. В организации 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 требованиям, 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 организации 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 организации незамедлительно.

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 организации обеспечивается доступ обучающихся и работников к:

4.2.1. 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;

4.2.2. общедоступным государственным и региональным информационным системам;

4.2.3. информационно-телекоммуникационной сети Интернет в порядке, установленном локальным нормативным актом организации.

4.3. В работе и (или) общении с обучающимися педагогическим работникам или иным работникам организации 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 организации.

4.4. Мониторинг содержания информационной продукции, используемой в образовательной деятельности педагогических работников осуществляется методическими объединениями, а также администрацией в рамках внутренней системы оценки качества образования.

4.5. В образовательной и (или) досуговой деятельности с обучающимися, организуемой и проводимой работниками организации, 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 организации 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 организации, несанкционированного доступа к локальной сети, а также обнаружении доступа к ресурсу, содержание которого может нанести вред здоровью и (или) развитию обучающихся, работники организации 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 организации 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 организации и (или) воспитанников и работников организации, 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 организации обеспечивается антивирусная защита компьютерной техники, систематически проводится обновление антивирусных программ.

5.3. Для приобретения и использования программного обеспечения в образовательной и иной деятельности организации проводится проверка его подлинности.

5.4. В организации с установленной периодичностью осуществляется контроль:

5.4.1. эксплуатации технических средств контентной фильтрации – постоянно, в организации используется контентная фильтрация провайдера МГТС (по договору);

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 организации – 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. функционирования системы антивирусной защиты – не реже 1 раза в месяц;

5.4.7. 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 организации не допускается обучающимися и работниками, а также иными лицами самовольная установка программного обеспечения на компьютерную технику организации, либо использование не принадлежащих организации программ и оборудования.

5.6. Мониторинг осуществления организационно-технических мер, направленных на обеспечение информационной безопасности учреждения осуществляется директором организации.

6. Заключительные положения

6.1. Положение вступает в силу с момента его утверждения.

6.2. 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.