МУНИЦИПАЛЬНОЕ КАЗЕННОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №7»
имени Николая Викторовича Кордюкова

Тел.: 8(48735)4-00-48
E-mail: school7.kimovsk@tularegion.org

301723, Тульская область, г. Кимовск,
улица Коммунистическая, дом 20-а

ПРИНЯТО:
педагогическим советом МКОУ «СОШ № 7»
протокол № 1 от 31.08.2023 г.

УТВЕРЖДАЮ:
Директор МКОУ «СОШ № 7»

_____Н.И. Ларюшкина
Приказ № 100 от 31.08.2023 г.

ПОЛОЖЕНИЕ
об информационной безопасности Муниципального казенного общеобразовательного учреждения «Средняя общеобразовательная школа № 7» имени Николая Викторовича Кордюкова

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1.Информационная безопасность в Муниципальном казенном общеобразовательном учреждении «Средняя общеобразовательная школа №7» имени Николая Викторовича Кордюкова (далее – Школа) – составное понятие, включающее технические, этические и правовые аспекты.

1.2.Законы, охватывающие вопросы информационной безопасности:

- Закон РФ «О безопасности» (от 05.03.1992 №2446-I) Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» (от 2.09.1992 № 3523-I)
- Закон РФ «Об авторском праве и смежных правах» (от 9.07.1993 №5351-I)
- Федеральный закон «Об информации, информатизации и защите информации» (от 20.02.1995 № 24-ФЗ)
- Федеральный закон «Об участии в международном информационном обмене» (от 04.07.1996 №85-ФЗ)
- Федеральный закон Российской Федерации о защите персональных данных от 27 июля 2006 года №152-ФЗ

1.3.Понятие информационной безопасности определено как «состояние защищенности информационной среды, общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства».

1.4.Целями защиты информационной сферы являются:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению модификации, искажению, копированию, блокированию информации;

· предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объема собственности;
· защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
· сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
· обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

1.5. Настоящее положение разработано в целях осуществления ограничения доступа обучающихся к ресурсам и материалам сети Интернет, не имеющих отношения к образовательному процессу.

1.6. Использование сети Интернет в Школе направлено на решение задач учебно-воспитательного процесса.

1.7. Настоящее Положение регулирует условия и порядок использования сети Интернет в Школе .

1.8. Настоящее Положение имеет статус локального нормативного акта Школы.

2. ОРГАНИЗАЦИЯ ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ В ШКОЛЕ

2.1. Положение вводится в действие приказом директора Школы.

2.2. Заместитель директора по УВР отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в Школе.

2.3. Во время уроков и других занятий в рамках учебного плана контроль использования обучающимися сети Интернет осуществляет учитель, ведущий занятие. При этом учитель:
- наблюдает за использованием компьютера и сети Интернет обучающимися;
- принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

2.4. При использовании сети Интернет в Школе обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношения к образовательному процессу. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации.

2.5. Пользователи сети Интернет в Школе должны учитывать, что технические средства и программное обеспечение не могут обеспечить полную фильтрацию ресурсов сети Интернет вследствие частого обновления ресурсов. В связи с этим существует вероятность обнаружения обучающимися ресурсов, не имеющих отношения к образовательному процессу и содержание которых противоречит законодательству Российской Федерации. Участникам использования сети Интернет в Школе следует осознавать, что Школа не несет ответственности за случайный доступ к подобной информации, размещенной не на Интернет-ресурсах Школы.

2.6. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в Школе правилами обеспечивается Советом по вопросам регламентации доступа к информации в сети Интернет.

2.7. Принципы размещения информации на Интернет-ресурсах Школы призваны обеспечивать:

• соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;

• защиту персональных данных обучающихся, их родителей (законных представителей), учителей и сотрудников;
• достоверность и корректность информации.

3. ИСПОЛЬЗОВАНИЕ СЕТИ ИНТЕРНЕТ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ

3.1. Использование сети Интернет в Школе осуществляется, как правило, в целях образовательного процесса.
3.2.По разрешению заместителя директора по УВР учителя, сотрудники вправе:
• размещать ссылки на собственные информационные ресурсы, связанные с образовательной деятельностью в сети Интернет, на Интернет-ресурсах Школы;
• иметь учетные записи на Интернет-ресурсах Школы.
3.3. Обучающимся запрещается:
• обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);
• осуществлять любые сделки через Интернет;
• осуществлять загрузки файлов на компьютеры Школы без специального разрешения;
• распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.
3.4. При случайном обнаружении ресурса, содержание которого не имеет отношения к образовательному процессу, обучающийся обязан незамедлительно сообщить об этом учителю, проводящему занятие. Учитель обязан зафиксировать доменный адрес ресурса и время его обнаружения и сообщить об этом заместителю директора по УВР.

4. ИСПОЛЬЗОВАНИЕ БИБЛИОТЕЧНЫХ ФОНДОВ

4.1 Заведующий библиотекой следит за обновлением Федерального списка экстремистских материалов, проводит проверку поступающей в библиотеку Школы литературы, периодических изданий и материалов согласно данному списку.
4.2 Проводит проверку библиотечного фонда Школы на предмет выявления литературы и материалов, содержащих информацию экстремистской направленности.

5. ОРГАНИЗАЦИЯ РАБОТЫ ОТВЕТСТВЕННОГО ЛИЦА ЗА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ШКОЛЫ

5.1. Ответственное лицо за информационную безопасность Школы назначается в целях выполнения требований действующего законодательства Российской Федерации, иных нормативно-правовых актов, регламентирующих обеспечение защиты информации, в том числе обеспечение безопасности при обработке персональных данных, а также обеспечение защиты и безопасности информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных.
5.2. Ответственное лицо за информационную безопасность Школы назначается приказом директора.
5.3. Ответственное лицо за информационную безопасность Школы осуществляет следующие функции:

- готовит и представляет проекты локальных нормативных актов по вопросам обеспечения защиты информации, в том числе персональных данных;
- для защиты информации, в том числе персональных данных от неправомерного доступа обеспечивает:

- контроль за строгим соблюдением доступа к конфиденциальной информации, в том числе к персональным данным;
- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения доступа к информации;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

- реализует меры по недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- реализует меры по информированию и обучению сотрудников по вопросам защиты информации и персональных данных;
- контролирует соблюдение парольной защиты; установленного регламента работы с электронной почтой; соблюдение требований к программному обеспечению и его использованию;
- обеспечивает ежегодное планирование работы по совершенствованию системы защиты информации.