МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ГОРОДА КАЛИНИНГРАДА ДЕТСКО-ЮНОШЕСКАЯ СПОРТИВНАЯ ШКОЛА ПО ХОККЕЮ С ШАЙБОЙ (МАУ ДО ДЮСШ ПО ХОККЕЮ С ШАЙБОЙ)

Приложение №2
к приказу № 181-О
от «26» сентября 2019 г.

УТВЕРЖДАЮ
Директор МАУ ДО ДЮСШ
по хоккею с шайбой
_____ Фёдорова В.И.
«26» сентября 2019 г.

Регламент
допуска сотрудников к обработке персональных данных в МАУ ДО ДЮСШ по хоккею с шайбой

1. Общие положения

1.1. Настоящий должностной регламент сотрудников (далее – Регламент) определяет основные цели, функции и права сотрудника по обеспечению безопасности персональных данных в МАУ ДО ДЮСШ по хоккею с шайбой (далее – Учреждение) .

1.2. Данный регламент составлен в соответствии с ФЗ-152 от 27.07.2006г., руководствуясь Постановлением №687 от 15.09.2008, постановлением №781 от 17.11.2007, устанавливает требования к обеспечению безопасности персональных данных при различных видах обработки.

1.3. Обработка персональных данных в учреждении может осуществляться только в функциональных и образовательных целях.

1.4. Допуск сотрудников осуществляющих хранение, обработку и передачу персональных данных определяется приказом директора учреждения.

1.5. Сотрудник проводи свою работу согласно нормативным документам в области обеспечения безопасности персональных данных.

1.6. Непосредственное руководство работой сотрудника осуществляет директор школы.

2. Основные функции сотрудника при обработке персональных данных

2.1. Проведение единой технической политики, организация и координация работ по обеспечению безопасности персональных данных в школе.

2.2. Проведение мероприятий по организации обеспечения безопасности персональных данных.

2.3. Проведение мероприятий по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в том числе

- мероприятия по размещению, охране, организации режима допуска в помещения, где ведётся обработка персональных данных;
- мероприятия по закрытию технических каналов утечки персональных данных при их обработке;
- мероприятия по защите от несанкционированного доступа к персональным данным;
- мероприятия по выбору средств защиты персональных данных при их обработке.

2.4. Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным или передачи их лицам, не имеющим права доступа к такой информации.

2.5. Своевременное обнаружение фактов несанкционированного доступа к персональным данным.

2.6. Недопущение воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование.

2.7. Обеспечение возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.8. Постоянных контроль за обеспечением уровня защищённости персональных данных.

2.9. Участие в подготовке объектов соответствующей организации к аттестации по выполнению требований обеспечения безопасности персональных данных.

2.10. Организация в установленном порядке расследования причин и условий появления нарушений в безопасности персональных данных и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений.

2.11. Разработка предложений, участие в проводимых работах по совершенствованию системы безопасности персональных данных в школе.

2.12. Проведение периодического контроля эффективности мер защиты персональных данных в учреждении. Учёт и анализ результатов контроля.

2.13. Организация повышения осведомленности руководства и сотрудников учреждения по вопросам обеспечения безопасности персональных данных.

3. Права сотрудников

Сотрудник имеет право:

3.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности персональных данных.

3.2. Разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных.

3.3. Готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.

3.4. Вносить предложения руководителю организации о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.

3.5. Привлекать в установленном порядке необходимых специалистов из числа сотрудников соответствующей организации для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.

4. Ответственность сотрудника

4.1. Сотрудник несёт персональную ответственность за:

- участие в передаче персональных данных, не определённой функциональными обязанностями и (или) запрещённой к передаче;
- искажение персональных данных при фиксации, передачи или копировании;
- использование персональных данных сотрудников и (или) учащихся, их законных представителей в целях, не предусмотренных должностными обязанностями; правильность и объективность принимаемых решений;
- правильное и своевременное выполнение приказов, распоряжений, указаний директора школы;
- выполнение возложенных на него обязанностей, предусмотренных настоящим Регламентом;
- соблюдение трудовой дисциплины, охраны труда;
- качество работы по обеспечению безопасности персональных данных;
- согласно действующему законодательству Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по раду работы.