



УТВЕРЖДЕНО
ПРИКАЗОМ
МАУДО "СШ №10"
от «17» июня 2026 г. № 129

ПРАВИЛА обработки персональных данных в ИСИДн

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила обработки персональных данных в информационных системах персональных данных (далее — Правила) устанавливают единый порядок работы с персональными данными при их обработке в информационных системах персональных данных в МУНИЦИПАЛЬНОМ АВТОНОМНОМ УЧРЕЖДЕНИИ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ГОРОДА НАБЕРЕЖНЫЕ ЧЕЛНЫ "СПОРТИВНАЯ ШКОЛА №10" (далее — Организация).

1.2. Правила разработаны в соответствии с требованиями:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказа Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных».

1.3. Настоящие Правила обязательны для исполнения всеми работниками Организации, имеющими доступ к информационным системам персональных данных.

1.4. В настоящих Правилах применяются термины и определения:

1.5. Контроль за соблюдением требований настоящих Правил возложен на:

- Директора Организации — в части организации обработки персональных данных;
- Заместителя директора — в части обеспечения безопасности персональных данных в информационных системах.

1.6. За нарушение требований настоящих Правил работники несут дисциплинарную, административную, уголовную и иную ответственность в соответствии с законодательством Российской Федерации.

Термин	Определение
Персональные данные (ПДн)	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Обработка персональных данных	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными

Информационная система персональных данных (ИСПДн)	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Оператор	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных
Субъект персональных данных	Физическое лицо, персональные данные которого обрабатываются оператором
Конфиденциальность персональных данных	Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта
Предоставление персональных данных	Действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц
Распространение персональных данных	Действия, направленные на раскрытие персональных данных неопределённому кругу лиц
Уничтожение персональных данных	Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных
Обезличивание персональных данных	Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту

2. ПОРЯДОК ДОСТУПА К ИСПДн

2.1. Доступ работников к информационным системам персональных данных предоставляется на основании приказа Директора Организации в объёме, необходимом для выполнения должностных обязанностей.

2.2. Перечень должностей работников, допущенных к обработке персональных данных в информационных системах:

- Директор;
- Заместитель директора по учебно-воспитательной работе;
- Заместитель директора по учебной работе;
- Инструктор-методист;
- Тренер-преподаватель;

2.3. Для каждого пользователя ИСПДн создаётся уникальная учётная запись с персональным именем пользователя и паролем. Использование групповых учётных записей запрещено.

2.4. Первичные пароли для доступа к ИСПДн выдаются Директором с обязательной регистрацией в журнале учёта паролей.

2.5. При изменении должности, увольнении работника или прекращении необходимости в доступе учётная запись блокируется в день издания соответствующего приказа.

2.6. Восстановление доступа при утрате пароля осуществляется Директором после идентификации личности работника.

2.7. Все операции по управлению учётными записями фиксируются в журнале учёта средств защиты информации.

3. ПРАВИЛА РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ В ИСПДн

3.1. При работе в информационных системах персональных данных пользователь обязан:

- использовать только свою персональную учётную запись;
- блокировать рабочую станцию при каждом покидании рабочего места;
- завершать сеанс работы в ИСПДн по окончании рабочего дня;
- немедленно сообщать Директору о любых подозрительных событиях и признаках несанкционированного доступа;
- соблюдать установленные требования парольной защиты.

3.2. Требования к паролям в ИСПДн:

- минимальная длина — 8 символов;
- обязательное использование букв верхнего и нижнего регистра, цифр и специальных символов;
- срок действия пароля — не более 90 дней;
- запрет на повторное использование последних 4 паролей;
- блокировка учётной записи после 5 неудачных попыток ввода пароля.

3.3. При работе в ИСПДн категорически запрещается:

- передавать свои учётные данные другим лицам;
- оставлять активную сессию без присмотра;
- записывать пароли на бумажных носителях или хранить в незащищённом виде;
- устанавливать программное обеспечение без согласования с Директором;
- изменять настройки средств защиты информации;
- подключать личные съёмные носители информации;
- копировать персональные данные на неучтённые носители.

4. ПОРЯДОК ВВОДА, ОБРАБОТКИ И ВЫВОДА ПДн

4.1. Ввод персональных данных в ИСПДн осуществляется уполномоченными работниками на основании первичных документов (заявлений, анкет, договоров, согласий на обработку).

4.2. При вводе персональных данных обеспечивается:

- проверка полноты и корректности вводимых данных;
- соответствие объёма вводимых данных заявленным целям обработки;
- контроль целостности и непротиворечивости данных.

4.3. Обработка персональных данных в ИСПДн осуществляется в следующих целях:

- Обеспечение реализации прав субъектов персональных данных (право на доступ, уточнение, удаление, отзыв согласия) (цель № 1);
- Обработка запросов Роскомнадзора, прокуратуры, суда и иных уполномоченных государственных органов (цель № 2);
- Обеспечение хранения документов, содержащих персональные данные, в соответствии с требованиями архивного законодательства (цель № 3);
- Осуществление кадрового учёта, обеспечение соблюдения трудового законодательства, принятие кадровых и управленческих решений в отношении работников (цель № 4);
- Ведение бухгалтерского учёта, исчисление и уплата налогов, расчёт и выплата заработной платы, предоставление налоговой и статистической отчётности (цель № 5);

- Обеспечение безопасных условий труда, проведение инструктажей, специальной оценки условий труда, расследование несчастных случаев (цель № 6);
- Ведение воинского учёта военнообязанных работников, предоставление сведений в военный комиссариат (цель № 7);
- Поиск и оценка кандидатов на замещение вакантных должностей (цель № 8);
- Исполнение судебных решений и постановлений, удержание из заработной платы по исполнительным документам (цель № 9);
- Размещение персональных данных работников на официальном сайте организации в информационно-телекоммуникационной сети Интернет (справочник сотрудников) (цель № 10);
- Передача персональных данных в удостоверяющий центр для выпуска сертификата ключа электронной подписи, оформление доверенностей (цель № 11);
- Заключение и исполнение договоров с организациями-контрагентами, ведение деловой переписки (цель № 12);
- Приём и рассмотрение обращений, жалоб и претензий клиентов, досудебное урегулирование споров (цель № 13);
- Продвижение товаров, работ, услуг путём осуществления прямых контактов с потенциальными потребителями с помощью средств связи (цель № 14);
- Обеспечение функционирования интернет-сайта и онлайн-сервисов организации, обработка файлов cookie, ведение статистики посещаемости (цель № 15);
- Обеспечение пропускного и внутриобъектового режима на территории и в помещениях оператора, контроль доступа (цель № 16);
- Выявление, предотвращение и расследование инцидентов информационной безопасности, уведомление Роскомнадзора об утечках (цель № 17);
- Ведение реестра членов организации, учёт членских взносов, обеспечение участия в управлении организацией (цель № 18);
- Осуществление закупочной деятельности, рассмотрение заявок участников, заключение контрактов (цель № 19);
- Организация и осуществление образовательной деятельности, зачисление, ведение учёта успеваемости, выдача документов об образовании (цель № 20);

4.4. Вывод персональных данных из ИСПДн (печать, экспорт, передача) допускается только:

- для исполнения договорных обязательств перед субъектом персональных данных;
- по запросу уполномоченных государственных органов;
- для передачи третьим лицам при наличии согласия субъекта или иных законных оснований.

4.5. Все операции по вводу, изменению и выводу персональных данных автоматически регистрируются в журнале событий ИСПДн с фиксацией:

- даты и времени операции;
- учётной записи пользователя;
- типа операции (создание, изменение, удаление, экспорт);
- идентификатора обрабатываемой записи.

5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПДн В ИСПДн

5.1. Для информационных систем персональных данных Организации установлен УЗ-3 (3-й уровень защищённости) при актуальных угрозах третьего типа.

5.2. Безопасность персональных данных при их обработке в ИСПДн обеспечивается применением:

- средств идентификации и аутентификации пользователей;
- средств разграничения доступа к информационным ресурсам;
- средств регистрации и учёта действий пользователей;
- средств антивирусной защиты;
- средств межсетевого экранирования;
- средств обнаружения вторжений;
- средств контроля целостности программного обеспечения.

5.3. При обработке персональных данных применяются средства криптографической защиты информации класса КС2, сертифицированные ФСБ России.

5.4. Резервное копирование баз данных ИСПДн выполняется:

- ежедневно — для оперативных данных;
- еженедельно — для полного резервного копирования;
- с хранением резервных копий в течение 30 дней.

5.5. Носители резервных копий хранятся в металлическом сейфе в помещении серверной с ограниченным доступом.

5.6. Техническое обслуживание средств вычислительной техники и программного обеспечения ИСПДн осуществляется только в присутствии Директора или уполномоченного им лица.

5.7. Контроль эффективности средств защиты информации проводится не реже одного раза в год с оформлением акта.

6. ДЕЙСТВИЯ ПРИ НЕШТАТНЫХ СИТУАЦИЯХ И ИНЦИДЕНТАХ

6.1. К нештатным ситуациям при обработке персональных данных в ИСПДн относятся:

- попытки несанкционированного доступа к персональным данным;
- нарушение функционирования средств защиты информации;
- обнаружение вредоносного программного обеспечения;
- утрата или компрометация учётных данных;
- сбои в работе программного обеспечения ИСПДн;
- физическое повреждение технических средств.

6.2. При обнаружении нештатной ситуации работник обязан:

- немедленно прекратить работу в ИСПДн;
- заблокировать рабочую станцию;
- не выключать и не перезагружать рабочую станцию (для сохранения следов инцидента);
- немедленно сообщить о произошедшем Директору;
- зафиксировать обстоятельства инцидента в журнале учёта нарушений.

6.3. Ответственное лицо при получении информации об инциденте:

- проводит первичную оценку ситуации;
- принимает меры по локализации инцидента;
- при необходимости привлекает технических специалистов;
- информирует Директора о серьёзных инцидентах.

6.4. Расследование инцидентов проводится в течение 3 рабочих дней с момента обнаружения с составлением акта расследования.

6.5. При выявлении инцидента, приведшего к неправомерному доступу к персональным данным, Организация в течение 24 часов направляет уведомление в Роскомнадзор, а в течение 72 часов — результаты внутреннего расследования.

7. КОНТРОЛЬ И ОТВЕТСТВЕННОСТЬ

7.1. Контроль за соблюдением настоящих Правил осуществляется:

- Директор — в части соблюдения порядка обработки персональных данных;
- Заместитель директора — в части выполнения требований по защите информации;
- Директор — общий контроль.

7.2. Проверка соблюдения требований настоящих Правил проводится:

- плановая — не реже одного раза в год;
- внеплановая — при выявлении нарушений или по указанию Директора.

7.3. Результаты проверок оформляются актом и доводятся до сведения Директора.

7.4. За нарушение требований настоящих Правил работники несут ответственность:

- дисциплинарную — в соответствии с Трудовым кодексом Российской Федерации;
- административную — в соответствии с Кодексом Российской Федерации об административных правонарушениях (статьи 13.11, 13.12, 13.13, 13.14);
- уголовную — в соответствии с Уголовным кодексом Российской Федерации (статьи 137, 272, 272.1);
- гражданско-правовую — в соответствии с Гражданским кодексом Российской Федерации.

7.5. Работник, допустивший нарушение требований настоящих Правил, может быть отстранён от работы с ИСПДн до прохождения внепланового инструктажа.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Настоящие Правила вступают в силу с момента их утверждения приказом Директора Организации.

8.2. Все работники, имеющие доступ к ИСПДн, должны быть ознакомлены с настоящими Правилами под подпись в листе ознакомления.

8.3. Изменения и дополнения в настоящие Правила вносятся приказом Директора по представлению ответственного лица или комиссии.

8.4. Пересмотр настоящих Правил проводится:

- при изменении законодательства Российской Федерации в области персональных данных;
- при изменении структуры или функций ИСПДн;
- по результатам проверок или аудита системы защиты персональных данных;
- но не реже одного раза в 3 года.

8.5. Ответственность за актуализацию настоящих Правил возложена на Директора.

8.6. Настоящие Правила подлежат хранению в течение 3 лет после замены новой версией.

ЛИСТ ОЗНАКОМЛЕНИЯ

С настоящим документом ознакомлен(а) и обязуюсь выполнять его требования:

№	Фамилия, имя, отчество	Должность	Дата	Подпись
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Лист согласования			Тип согласования: последовательное	
N°	ФИО	Срок согласования	Результат согласования	Замечания
1	Зайнеева О.В.		 Подписано 06.07.2026 - 13:23	-