АМИНИСТРАЦИЯ ТУРИНСКОГО МУНИЦИПАЛЬНОГО ОКРУГА
СВЕРДЛОВСКОЙ ОБЛАСТИ

МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«УПРАВЛЕНИЕ ОБРАЗОВАНИЕМ ТУРИНСКОГО МУНИЦИПАЛЬНОГО ОКРУГА»
(МКУ «УПРАВЛЕНИЕ ОБРАЗОВАНИЕМ»)

Муниципальное автономное дошкольное образовательное учреждение
Детский сад № 5 «Огонёк»

Приказ

13.04.2026г. **№ 103-П**

г. Туринск

О назначении ответственных лиц за организацию обработки персональных данных и обеспечении их защиты

С целью оказания услуг в сфере дошкольного образования, осуществления сбора и анализа информации, создания базы данных в системе образования, в соответствии с Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных» (с изменениями на 1 сентября 2025 года); Федеральным законом от 24 июня 2025 года №156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации»; Уставом Муниципального автономного дошкольного образовательного учреждения Детский сад №5 «Огонёк»,

ПРИКАЗЫВАЮ:

1.Назначить ответственными за организацию обработки персональных данных обеспечения их защиты:

1.1. Перминову Т. А., заведующего МАДОУ Детский сад № 5 «Огонёк» — в части общего руководства и контроля за обработкой и защитой персональных данных в учреждении, включая:

- утверждение локальных нормативных актов по обработке персональных данных;
- организацию взаимодействия с надзорными органами;
- контроль за соблюдением требований законодательства о персональных данных;
- принятие решений о внедрении новых информационных систем обработки данных.

1.2. Плотникову А. В., заместителя заведующего:

- за обработку персональных данных педагогических работников в части аттестации и повышения квалификации в рамках автоматизированной информационной системы КАИС ИРО и других систем которые необходимы в процессе работы.

• за работу с персональными данными воспитанников в рамках автоматизированной информационной системы «Навигатор» и других систем которые необходимы в процессе работы.

•разработку внутренних документов по защите персональных данных;

•ведение учёта в автоматизированных информационных системах.

1.3. Грицай Т.В., делопроизводителя — за обработку персональных данных сотрудников, воспитанников и их законных представителей в части:

•кадрового учета;

•договорной работы;

•передачи данных в государственные информационные системы.

2.Определить следующие обязанности ответственных лиц:

2.1. Перминова Т. А. обязана:

•организовывать общую работу по обработке и защите персональных данных в учреждении;

•утверждать локальные нормативные акты по обработке персональных данных;

•обеспечивать взаимодействие с уполномоченным органом по защите прав субъектов персональных данных;

•контролировать соблюдение требований по защите персональных данных всеми работниками учреждения;

•проводить регулярные проверки соблюдения требований законодательства о персональных данных;

•принимать меры по устранению выявленных нарушений;

•обеспечивать своевременное обновление средств защиты информации;

•организовывать обучение работников правилам обработки и защиты персональных данных.

2.2. Плотникова А.В. обязана:

•организовывать обработку персональных данных педагогов;

•вести учет в автоматизированных информационных системах;

•контролировать соблюдение требований по аттестации педагогических работников;

•обеспечивать безопасность персональных данных при работе с информационными системами;

•обрабатывать запросы субъектов персональных данных;

•осуществлять работу в автоматизированной информационной системе КАИС ИРО;

•осуществлять работу в автоматизированной информационной системе «Навигатор» включая ввод, обновление и верификацию данных воспитанников (ФИО, дата рождения, СНИЛС, номер сертификата персонифицированного финансирования дополнительного образования, контактные данные)

•разрабатывать внутренние документы по защите персональных данных.

2.3. Грицай Т.В. обязана:

- организовывать обработку персональных данных сотрудников, включая сбор, обработку и хранение данных, необходимых для кадрового учёта, оформления трудовых договоров и других кадровых процедур;
- оформлять трудовые договоры и личные дела сотрудников, вести их учёт, обеспечивать сохранность документов;

- осуществлять взаимодействие с государственными информационными системами: системой обязательного пенсионного страхования, системой социального страхования, ЕГИССО, ГИС СО, системой электронного документооборота и другие;
- оформлять договоры с родителями (законными представителями) на оказание образовательных услуг;
- передавать данные о льготных категориях детей в ЕГИССО;
- обеспечивать защиту персональных данных при работе в информационных системах, соблюдать конфиденциальность;
- контролировать соблюдение требований законодательства о персональных данных;
- вести учет и хранение кадровой документации;
- обеспечивать своевременное предоставление отчетности в государственные органы;
- контролировать актуальность персональных данных сотрудников в информационных системах;
- осуществлять обезличивание данных при передаче в государственные информационные системы в соответствии с требованиями законодательства;
- вести учет операций по обезличиванию персональных данных.

3.Установить следующие требования:

3.1. Доступ к персональным данным предоставляется только:

- лицам, указанным в настоящем приказе;
- работникам учреждения в пределах их должностных обязанности.

3.2. Запретить:

- передачу персональных данных третьим лицам без согласия субъектов персональных данных;
- использование иностранных облачных сервисов для хранения персональных данных;
- размещение персональных данных в открытых источниках;
- обработку обезличенных данных вне установленных законодательством систем.

3.3. Обеспечить:

- размещение баз данных с персональными данными на территории РФ;
- регулярное проведение аудита систем обработки персональных данных;
- своевременное обновление средств защиты информации;
- соблюдение порядка обезличивания данных при передаче в государственные информационные системы;
- ведение журнала учета операций по обезличиванию данных.

4. Утвердить Инструкцию ответственного за организацию обработки персональных данных (Приложение №1 к настоящему приказу), Инструкцию по обеспечению безопасности персональных данных в информационных системах (Приложение №2 к настоящему приказу)

5. Обеспечить ознакомление ответственных лиц с инструкциями, являющимися приложениями к настоящему приказу, под подпись в течение 3 рабочих дней с момента утверждения

6. Заместителю заведующей разместить настоящий приказ и приложения к нему на официальном сайте Учреждения в течение 5 дней со дня издания приказа

7.Контроль за исполнением настоящего приказа оставляю за собой.

Заведующий Т.А. Перминова

С приказом «О назначении ответственных лиц за организацию обработки персональных данных и обеспечении их защиты» от 13.04.2026 № 103-П ознакомлены:

№ п/п	Дата	ФИО	Должность	Подпись
1		Грицай Татьяна Васильевна	Делопроизводитель	
2		Плотникова Анна Васильевна	Заместитель заведующего	
3		Перминова Татьяна Александровна	Заведующий	

Приложение № 1
К приказу от 13.04.2026 № 103-П

ИНСТРУКЦИЯ
ответственного лица за организацию обработки персональных данных и обеспечении их защиты
в Муниципальное автономное дошкольное образовательное учреждение
Детский сад № 5 «Огонёк»

1. Термины и определения

1.1. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.2. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.3. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

1.4. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция определяет функции, права и ответственность ответственного за организацию обработки персональных данных (далее по тексту – Ответственный) в Муниципальном автономном дошкольном образовательном учреждении Детский сад № 5 «Огонёк (далее по тексту–Учреждение).

2.2. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных (далее по тексту – ПДн), не исключает обязательного выполнения их требований.

2.3. Ответственный назначается приказом заведующей Учреждения.

2.4. Ответственный непосредственно подчиняется заведующей Учреждения.

2.5. На время отсутствия (болезнь, отпуск, пр.) Ответственного его обязанности возлагаются на работника, назначенного и допущенного в установленном порядке.

3. Функциональные обязанности

3.1. Ответственный выполняет следующие функции:

- осуществляет внутренний контроль за соблюдением работниками, обрабатывающими ПДн в информационных системах персональных данных (далее по тексту–ИСПДн) и без использования средств автоматизации требований законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;
- взаимодействует с уполномоченными органами государственной власти Российской Федерации, органами по аттестации, испытательными лабораториями по вопросам обработки и защиты ПДн (при проведении государственного контроля и надзора, аттестации, сертификации);
- актуализирует перечень должностей работников, имеющих доступ к обработке ПДн;
- актуализирует перечень работников, допущенных в помещения, в которых осуществляется обработка ПДн;
- доводит до сведения работников, обрабатывающих ПДн положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите

ПДн, в том числе требований к защите ПДн;

- организовывает прием и обработку обращений и запросов субъектов ПДн или их представителей, чьи ПДн обрабатываются в Учреждении, или их представителей, и осуществляет контроль за приемом и обработкой таких обращений и запросов;
- разрабатывает и корректирует эксплуатационную документацию и организационно-распорядительные документы по защите ПДн;
- принимает участие в деятельности по подготовке, пересмотру, уточнению локальных актов по защите информации; по аттестации объектов информатизации;
- организует и проводит регулярный аудит систем обработки персональных данных, включая проверку эффективности применяемых мер защиты и соответствия обработки установленным требованиям;
- осуществляет постоянный мониторинг изменений в законодательстве Российской Федерации в сфере защиты персональных данных и информирует руководство о необходимости внесения соответствующих изменений в локальные акты;
- ведет журнал регистрации инцидентов, связанных с нарушением безопасности персональных данных, включая фиксацию обстоятельств, причин и последствий инцидентов, а также принятых мер по их устранению;
- контролирует соблюдение установленных сроков хранения персональных данных, их своевременную актуализацию и корректное уничтожение по истечении срока хранения;
- организует и контролирует процессы резервного копирования персональных данных, включая: разработку регламентов резервного копирования, проверку работоспособности резервных копий, обеспечение их сохранности и конфиденциальности, своевременное обновление процедур резервного копирования.

4. Права

4.1. Ответственный имеет право:

- требовать от работников, обрабатывающих ПДн, соблюдения установленной технологии обработки ПДн и выполнения инструкций по обеспечению безопасности информации;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, уничтожения ПДн и технических средств, обрабатывающих ПДн;
- требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;
- подавать свои предложения по, совершенствованию организационных и технических мер по защите ПДн.

5. Ответственность

5.1. На Ответственного возлагается персональная ответственность за качество выполняемых им функций по обеспечению защиты ПДн.

5.2. Ответственный несет ответственность по действующему законодательству Российской Федерации за разглашение сведений ограниченного доступа, ставших ему известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6. Срок действия и порядок внесения изменений

6.1. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.

6.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

6.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом заведующей Учреждения.

Приложение № 2
К приказу от 13.04.2026 № 103-П

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в Муниципальном автономном дошкольном образовательном учреждении Детский сад № 5 «Огонёк»

1. Термины и определения

1.1. Доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие право доступа к информации в соответствии с локальными актами и законодательством Российской Федерации, могут беспрепятственно реализовывать данное право.

1.2. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.3. Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

1.4. Конфиденциальность информации – свойство безопасности информации, при котором доступ к информации осуществляют только те субъекты доступа, которые имеют на это право в соответствии с локальными актами и законодательством Российской Федерации.

1.5. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.6. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

1.7. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

1.8. Целостность информации – свойство безопасности информации, при котором изменение информации осуществляют только те субъекты доступа, которые имеют на это право в соответствии с локальными актами и законодательством Российской Федерации.

2. Общие положения

2.1. Настоящая Инструкция определяет функции, обязанности и права ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее по тексту – Ответственный) в Муниципальном автономном дошкольном образовательном учреждении Детский сад № 5 «Огонёк» (далее по тексту- Учреждение)

2.2. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных (далее по тексту – ПДн), не исключает обязательного выполнения их требований.

2.3. Ответственный назначается приказом заведующей Учреждения.

2.4. На время отсутствия (болезнь, отпуск, пр.) Ответственного его обязанности возлагаются на работника, назначенного и допущенного в установленном порядке.

3. Функциональные обязанности

3.1. Ответственный выполняет следующие функции:

3.1.1. Управляет доступом пользователей в ИСПДн;

3.1.2. Управляет полномочиями пользователей в ИСПДн;

3.1.3. Поддерживает установленные правила разграничения доступа в ИСПДн;

3.1.4. Управляет (администрирует) системой защиты информации (далее – СиЗИ) ИСПДн:

- управляет средствами защиты информации (далее – СЗИ)
- управляет программным обеспечением СЗИ;
- восстанавливает работоспособность СЗИ;
- устанавливает обновления программного обеспечения СЗИ, выпускаемых разработчиками (производителями) СЗИ;
- анализирует события в ИСПДн, связанные с защитой информации (события безопасности);
- информирует пользователей об угрозах безопасности информации;
- информирует пользователей о правилах эксплуатации СЗИ;
- обучает пользователей работе со СЗИ;
- управляет доступом к съемным машинным носителям информации, используемым в ИСПДн (определяет должностных лиц, имеющих доступ к съемным машинным носителям информации);
- сопровождает функционирование СиЗИ в ходе ее эксплуатации;
- поддерживает конфигурацию СиЗИ (структуру СиЗИ, состав, места установки и параметры настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на СиЗИ (поддержание базовой конфигурации СиЗИ);
- определяет лиц, которым разрешены действия по внесению изменений в базовую конфигурацию СиЗИ;
- управляет изменениями базовой конфигурации СиЗИ, в том числе:
- определяет типы возможных изменений;
- разрешает или отказывает во внесении изменений;
- документирует действия по внесению изменений;
- хранит данные об изменениях.

3.1.5. Поддерживает конфигурацию ИСПДн (структуру ИСПДн, состав, места установки и параметры программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на ИСПДн;

3.1.6. Анализирует потенциальные воздействия планируемых изменений в базовой конфигурации СиЗИ на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПДн;

3.1.7. Определяет параметры настройки программного обеспечения, включая программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИСПДн и СиЗИ;

3.1.8. Выявляет инциденты (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИСПДн и (или) к возникновению угроз безопасности информации (далее– Инциденты), и реагирует на них.

3.1.9. Обнаруживает и идентифицирует Инциденты, в том числе:

- отказы в обслуживании;
- сбои (перезагрузки) в работе СЗИ;
- нарушения правил разграничения доступа;
- неправомерные действия по сбору информации;
- иные события, приводящие к возникновению Инцидентов.

3.1.10. Анализирует Инциденты, в том числе определяет источники и причины возникновения Инцидентов, а также оценивает их последствия;

3.1.11. Планирует меры по устранению Инцидентов, в том числе:

- по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев;
- устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению Инцидентов.

3.1.12. Планирует и принимает меры по предотвращению повторного возникновения Инцидентов.

3.1.13. Контролирует обеспечение уровня защищенности ПДн, обрабатываемых в ИСПДн:

- контролирует события безопасности и действия пользователей в ИСПДн;
- контролирует (анализирует) уровень защищенности ПДн;
- контролирует перемещение съемных машинных носителей информации за пределы контролируемой зоны лицами, которым оно необходимо для выполнения своих должностных обязанностей (функции);
- анализирует и оценивает функционирование СиЗИ ИСПДн, включая выявление, анализ и устранение недостатков в функционировании СиЗИ ИСПДн;
- выполняет периодический анализ изменения угроз безопасности ПДн в ИСПДн, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности ПДн;
- документирует процедуры и результаты контроля (мониторинга) за обеспечением уровня защищенности ПДн, содержащихся в ИСПДн;
- принимает решения по результатам контроля (мониторинга) за обеспечением уровня защищенности ПДн о доработке (модернизации) СиЗИ ИСПДн.

3.1.14. Ведет учет:

- используемых шифровальных (криптографических) СЗИ в ИСПДн, эксплуатационной и технической документации к ним;
- съемных машинных носителей (при их наличии), используемых в ИСПДн для хранения и обработки ПДн.

3.1.15. Обеспечивает защиту информации при выводе из эксплуатации ИСПДн или после принятия решения об окончании обработки информации:

- обеспечивает архивирование информации, содержащейся в ИСПДн (архивирование должно осуществляться при необходимости дальнейшего использования);
- обеспечивает уничтожение (стирание) данных и остаточной информации со съемных машинных носителей информации, при необходимости передачи съемного машинного носителя информации другому пользователю ИСПДн или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения;
- при выводе из эксплуатации съемных машинных носителей информации, на которых осуществлялись хранение и обработка ПДн, осуществляет физическое уничтожение этих съемных машинных носителей информации.

4. Права

4.1. Ответственный имеет право:

- требовать от работников – пользователей ИСПДн соблюдения установленной технологии обработки ПДн и выполнения требований локальных нормативных актов и иной организационно-распорядительной документации по обеспечению безопасности ПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи информации ограниченного доступа и технических средств, входящих в состав ИСПДн;
- требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования СиЗИ;
- участвовать в анализе ситуаций, касающихся функционирования СЗИ и расследования фактов несанкционированного доступа к ПДн;
- подавать свои предложения по совершенствованию организационных и технических мер по защите ПДн.

5. Ответственность

5.1. Ответственному категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных (личных) целях;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках СЗИ, которые могут привести к инцидентам информационной безопасности.

5.2. На Ответственного возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты ПДн.

5.3. Ответственный несет ответственность по действующему законодательству за разглашение сведений ограниченного доступа, ставших ему известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6. Срок действия и порядок внесения изменений

6.1. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.

6.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

6.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом заведующей Учреждения.