ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДЕТСКИЙ САД № 45
ПУШКИНСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА
196634 Санкт-Петербург, поселок Шушары, Славянка, Ростовская улица, дом 25, корпус 1, литер А
телефон/факс 8(812)320-40-80, 320-40-81

ПРИНЯТО
Общим собранием работников
Образовательного учреждения
Решение протокола от 26.08.2021 №1

УТВЕРЖДЕНО
Приказом от 26.08.2021 №105-О

Заведующий **Е.В. Акулич**

Учтено мнение родителей
(законных представителей)
воспитанников ***от 09.06.2021***

Заведующий
Акулич Елена
Владимировна

Подписано цифровой подписью: Заведующий Акулич Елена Владимировна
Дата: 2022.06.17 12:55:25 +03'00'

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ВОСПИТАННИКОВ И ИХ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ)

(новая редакция)

САНКТ-ПЕТЕРБУРГ
2021

I. Общие положения

1.1. Настоящее **Положение о защите персональных данных воспитанников и их родителей (законных представителей)** в государственном бюджетном дошкольном образовательном учреждении детском саду № 45 Пушкинского района Санкт-Петербурга (далее - образовательное учреждение, ОУ) разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Уставом образовательного учреждения, с учетом Постановления Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средства автоматизации», с учетом Постановления Правительства РФ от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
1.2.Данное Положение о защите персональных данных воспитанников и их родителей (законных представителей) (далее -Положение) определяет основные требования к порядку получения, хранения, использования и передачи персональных данных воспитанников, родителей детей, а также ответственность за нарушение норм, регулирующих обработку и защиту персональных данных в образовательном учреждении.
1.3. Положение устанавливает основные понятия и состав персональных данных воспитанников и их родителей (законных представителей) в ОУ, регламентирует формирование и ведение личных дел, определяет права и обязанности работников по защите персональных данных, права родителей (законных представителей) воспитанников по обеспечению защиты персональных данных своих детей, а также обязанности родителей (законных представителей) по обеспечению достоверности персональных данных.
1.4.Целью настоящего Положения является обеспечение защиты в ОУ прав и свобод участников образовательных отношений при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.
1.5.Обязанность предоставления персональных данных родителем (законным представителем) воспитанника предусмотрена федеральными законами, ОУ разъясняет юридические последствия отказа от предоставления своих персональных данных и персональных данных своего ребенка.
1.6.При определении объема и содержания персональных данных воспитанника и родителя (законного представителя) администрация ОУ руководствуется Конституцией Российской Федерации, федеральными законами и настоящим Положением.
1.7.Настоящее Положение является локальным нормативным актом ОУ. Положение является обязательным для исполнения всеми работниками в образовательном учреждении, имеющими доступ к персональным данным воспитанников и их родителей (законных представителей).

II. Основные понятия и состав персональных данных воспитанников и их родителей (законных представителей)

2.1.***Персональные данные*** — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;
2.2.***Оператор*** — юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
2.3.***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.
2.4.***Автоматизированная обработка персональных данных*** — обработка персональных данных с помощью средств вычислительной техники.
2.5.***Распространение персональных данных*** — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
2.6.***Предоставление персональных данных*** — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
2.7.***Блокирование персональных данных*** — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
2.8.***Уничтожение персональных данных*** — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.9.***Обезличивание персональных данных*** — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
2.10.***Информационная система персональных данных*** — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
2.11.***Общедоступные данные*** — сведения общего характера и иная информация, доступ к которой не ограничен.
2.12.Персональные данные воспитанников, родителей (законных представителей), являются информацией, доступ к которой ограничен по закону и которая может быть получена, использована и распространена работниками образовательного учреждения лишь с соблюдением установленного порядка.
2.13.К персональным данным воспитанника и его родителей (законных представителей) относятся:

- *сведения, содержащиеся в свидетельстве о рождении ребенка;*
- *паспортные данные родителя (законного представителя);*
- *данные, подтверждающие законность представления прав воспитанника;*
- *сведения о воспитаннике, лишенного родительского попечения;*
- *сведения о регистрации и проживании воспитанника;*
- *сведения о состоянии здоровья воспитанника;*
- *данные страхового медицинского полиса;*
- *данные страхового номера индивидуального лицевого счета (СНИЛС) воспитанника;*
- *фотографии ребенка;*
- *контактные телефоны родителей (законных представителей);*
- *сведения о месте работы (учебы) родителей (законных представителей) воспитанника;*
- *информация, имеющая отношение к предоставлению льготы за содержание воспитанника в образовательном учреждении;*
- *информация о банковском счете родителей воспитанников (законных представителей) для возврата не использованных денежных средств (переплаты) за содержание воспитанников в ДОУ;сведения о доходах семьи;*
- *иные сведения, необходимые для определения отношений обучения и воспитания.*

2.14.При оформлении ребенка, родитель (законный представитель) представляет следующие документы:

- *Форму направления, выданное Комиссией по комплектованию дошкольных образовательных учреждений Пушкинского района Санкт-Петербурга;*
- *Свидетельство о рождении ребенка;*
- *Документ, удостоверяющий личность заявителя;*
- *Документ, подтверждающий право заявителя действовать в интересах ребенка;*
- *Документ удостоверяющий личность ребенка, выданный компетентными органами иностранного государства, и его нотариально удостоверенный перевод на русский язык;*
- *Документы, подтверждающие право на внеочередное право зачисления ребенка или документ, подтверждающий право на первоочередное право зачисления ребенка;*
- *Документ о регистрации брака;*
- *Постановление об установлении опеки, доверенность на представление интересов ребенка (при наличии);*
- *Документ, подтверждающий регистрацию воспитанника;*
- *Другие сведения, необходимые о состоянии здоровья воспитанника (медицинское заключение (медицинская карта ребенка)).*

2.15.Для проведения в полном объеме медицинского обслуживания воспитанника в ОУ его родитель (законный представитель) представляет копию страхового медицинского полиса воспитанника. Медицинская карта и прививочный сертификат воспитанника содержатся у медицинского работника медицинской организации закрепленной за ОУ.
2.16.Для зачисления ребенка в группу компенсирующей направленности родитель (законный представитель) представляет оригинал выписки коллегиального заключения психолого-медико-педагогической комиссии с соответствующими рекомендациями (**Заключение психолого-медико-педагогической комиссии).**
2.17.Личное дело воспитанника находится в документации заведующего и состоит из следующих документов:

- *форма направления;*
- *заявление родителей (законных представителей) о приёме в образовательное учреждение;*
- *копия свидетельства о рождении ребёнка;*
- *копия документа, удостоверяющий личность заявителя;*
- *согласие на обработку персональных данных;*
- *договор об образовании по образовательным программам между ОУ и родителями (законными представителями) ребёнка;*
- *документы, подтверждающие право на внеочередное право зачисления ребенка или документ, подтверждающий право на первоочередное право зачисления ребенка (при наличии).*

2.18.Сбор сведений для компенсаций части родительской платы за содержание ребёнка в ОУ, установлено действующим законодательством, родитель (законный представитель). При сборе сведений о воспитаннике,

установленных действующим законодательством, родитель (законный представитель), предоставляет копии документов, подтверждающих законность представления прав ребёнка:

- *копия документа, удостоверяющий личность заявителя;*
- *копия свидетельства о рождении ребёнка;*
- *постановление об установлении опеки, доверенность на представление интересов воспитанника;*
- *свидетельства о браке или разводе (при разных фамилиях ребёнка и родителя);*
- *копия справки об инвалидности;*
- *копия удостоверения многодетной матери;*
- *Другие сведения (справки о доходах, свидетельства о рождении детей проживающих в семье, свидетельство о разводе и т.д.), необходимые для подтверждения льготы.*

2.19.Размещение на официальном сайте ОУ воспитанников и их родителей (законных представителей), фото и видеосъемку праздников в образовательном учреждении родители (законные представители) разрешают по письменному согласию.

2.20.Размещение в групповых родительских уголках фотографий воспитанников и их родителей (законных представителей), фото и видеосъемку праздников в образовательном учреждении родители (законные представители) разрешают по письменному согласию.

2.21.Работники ОУ могут получить от самого воспитанника данные:

- *о фамилии, имени, отчестве, дате рождения и месте жительстве воспитанника;*
- *о фамилии, имени, отчестве родителей (законных представителей) воспитанника.*

2.22.Иные персональные данные воспитанника, необходимые в связи с отношениями образования и воспитания, администрация ОУ может получить с письменного согласия одного из родителей (законного представителя). В случаях, когда администрация ОУ может получить необходимые персональные данные воспитанника только у третьего лица, администрация ОУ уведомляет об этом одного из родителей (законного представителя) заранее и получить от него письменное согласие. Администрация ОУ обязана сообщить одному из родителей (законному представителю) воспитанника о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа одного из родителей (законного представителя) дать письменное согласие на их получение.

2.23.Персональные данные воспитанника и родителя (законного представителя) ребенка являются конфиденциальной информацией и не могут быть использованы работниками образовательного учреждения в личных целях.

2.24.Образовательное учреждение определяет объем, содержание обрабатываемых персональных данных воспитанников, руководствуясь Конституцией Российской Федерации, данным Положением, Уставом ОУ и иными федеральными законами.

III. Порядок получения, обработки, хранения персональных данных

3.1.Обработка персональных данных воспитанника ОУ осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов в целях воспитания и обучения воспитанника, обеспечения его личной безопасности, контроля качества образования, пользования льготами, предусмотренными законодательством Российской Федерации и локальными актами администрации образовательного учреждения.

3.2.Порядок получения персональных данных воспитанников, родителей (законных представителей):

3.2.1.Родитель (законный представитель) предоставляет заведующему или работнику, имеющему допуск к персональным данным воспитанника (оператору), достоверные сведения о себе и своём ребёнке, а также оригиналы и копии требуемых документов.

3.2.2.Заявление о приеме в ОУ и прилагаемые к нему документы, представленные родителями (законными представителями) воспитанников, регистрируются заведующим или сотрудником, имеющим допуск к персональным данным детей (оператором), в журнале приема заявлений. После регистрации заявления родителям (законным представителям) выдается расписка с перечнем принятых копий документов.

3.2.3. Все персональные данные воспитанника, родителей (законных представителей) получает заведующий или сотрудник, имеющим допуск к персональным данным детей (оператором), а родитель (законный представитель) передает лично. Если персональные данные воспитанника, родителей (законных представителей) возможно, получить только у третьей стороны, то родитель (законный представитель) должен быть уведомлен об этом заранее письменно (ПРИЛОЖЕНИЕ №2).

3.2.4.Заведующий ОУ обязан сообщить одному из родителей (законному представителю) о целях, способах, и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа одного из родителей (законного представителя) дать письменное согласие на их получение (ПРИЛОЖЕНИЕ №3).

3.2.5.Работник образовательного учреждения (оператор) не имеет права получать и обрабатывать персональные данные воспитанника и родителя (законного представителя) о их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

3.2.6.Согласие родителя (законного представителя) на обработку своих персональных данных и своего ребёнка

может быть отозвано путем направления родителем (законным представителем) письменного заявления не менее чем за 3 дня до момента отзыва (ПРИЛОЖЕНИЕ №4).

*3.2.7.**Согласие родителя (законного представителя) не требуется в следующих случаях:***

- *обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;*
- ***обработка персональных данных осуществляется в соответствии с Федеральными законами;***
- *обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;*
- *обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;*
- ***обработка персональных данных осуществляется в целях оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;***
- *обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;*
- *обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;*
- *обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;*
- ***обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;***
- ***обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;***
- *обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;*
- ***обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.***

3.3.Принципы обработки персональных данных воспитанников и родителей (законных представителей):

- *законности целей и способов обработки персональных данных и добросовестности;*
- *соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям работника, осуществляющего обработку персональных данных в образовательном учреждении;*
- *соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;*
- *достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;*
- *недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.*

3.4.Порядок обработки, передачи и хранения персональных данных:

3.4.1.Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения или продлевается на основании заключения экспертной комиссии образовательного учреждения, если иное не определено законом.

3.4.2.При передаче персональных данных воспитанника и родителя (законного представителя) заведующий ОУ или работник (оператор), имеющий допуск к персональным данным, должен соблюдать следующие требования:

- *не сообщать персональные данные воспитанника или родителя (законного представителя) третьей стороне без письменного согласия за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью воспитанника или родителя (законного представителя), а также в случаях, установленных федеральными законами Российской Федерации;*
- *предупредить лиц, получивших персональные данные воспитанника или родителя (законного представителя), о том, что эти данные могут быть использованы лишь в целях, для которых они*

сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные воспитанника или родителя (законного представителя) ребенка, обязаны соблюдать режим секретности (конфиденциальности);

- *разрешать доступ к персональным данным воспитанника или родителя (законного представителя) только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные воспитанника ОУ или родителя (законного представителя), которые необходимы для выполнения конкретной функции.*

3.4.3.Хранение и использование документированной информации персональных данных воспитанника или родителя (законного представителя):

- *персональные данные воспитанника или родителя (законного представителя) ребенка могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде;*
- *персональные данные воспитанников и родителей (законных представителей) хранятся в местах с ограниченным доступом к этим документам;*
- *персональные данные воспитанника и родителей (законных представителей) хранятся в ОУ с момента их внесения в базу данных и до выпуска из образовательного учреждения.*

3.5.При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

3.6.Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3.7.Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.8.Оператор при обработке персональных данных обеспечивает безопасность персональных данных, с применением организационных и технических мер (ПРИЛОЖЕНИЕ №1) по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных.

3.8.1.Оператор при обработке персональных данных применяет меры (ПРИЛОЖЕНИЕ №1) *по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий:*

№ п/п	**Меры по обеспечению безопасности персональных данных**	
1.	идентификация и аутентификация субъектов доступа и объектов доступа;	Меры должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).
2.	управление доступом субъектов доступа к объектам доступа;	Меры должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.
3.	ограничение программной среды;	Меры должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.
4.	защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;	Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

5.	регистрация событий безопасности;	Меры должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.
6.	антивирусная защита;	Меры должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.
7.	обнаружение (предотвращение) вторжений;	Меры должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.
8.	контроль (анализ) защищенности персональных данных;	Меры должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.
9.	обеспечение целостности информационной системы и персональных данных;	Меры должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.
10.	обеспечение доступности персональных данных;	Меры должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.
11.	защита среды виртуализации;	Меры должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.
12.	защита технических средств;	Меры должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.
13.	защита информационной системы, ее средств, систем связи и передачи данных;	Меры должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности

		персональных данных.
14.	выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;	Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.
15.	управление конфигурацией информационной системы и системы защиты персональных данных.	Меры должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

3.8.2.Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении 1 к настоящему Положению.

IV. Доступ к персональным данным воспитанников и родителей (законных представителей)

4.1.Право доступа к персональным данным воспитанников и их родителей (законных представителей) имеют:
заведующий ОУ; исполняющий обязанности заведующего ОУ;
заместитель заведующего по учебно-воспитательной работе;старший воспитатель;
заместитель заведующего по административно-хозяйственной части, заведующий хозяйством;
главный бухгалтер (бухгалтер);
медицинский работник;
воспитатель;
специалист (учитель-логопед, педагог дополнительного образования, педагог-психолог, другие специалисты музыкальный руководитель;инструктор по физической культуре;);
документовед, делопроизводитель.
4.2.Каждый из вышеперечисленных сотрудников образовательного учреждения даёт расписку (ПРИЛОЖЕНИЕ №5) о неразглашении персональных данных. Расписки хранятся в одном деле с оригиналом настоящего Положения. По мере смены должностных лиц эти обязательства должны обновляться.
4.3.В целях обеспечения надлежащего выполнения трудовых обязанностей доступ к персональным данным воспитанника или родителя (законного представителя) может быть предоставлен на основании приказа заведующего ОУ иному работнику, должность которого не включена в список лиц, уполномоченных на получение и доступ к персональным данным.
4.4.Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных воспитанников, определяются трудовыми договорами и должностными инструкциями.

V. Обязанности работников (операторов), имеющих доступ к персональным данным воспитанников

5.1.Работники ОУ (операторы), имеющие доступ к персональным данным воспитанников, ***обязаны***:

- *не сообщать персональные данные воспитанника третьей стороне без письменного согласия одного из родителей (законного представителя) ребенка, кроме случаев, когда в соответствии с Федеральными законами такого согласия не требуется;*
- *использовать персональные данные воспитанника, полученные только от него лично или с письменного согласия одного из родителей (законного представителя) ребенка;*
- *обеспечить защиту персональных данных воспитанника от их неправомерного использования или утраты, в порядке, установленном законодательством Российской Федерации;*
- *соблюдать требование конфиденциальности персональных данных воспитанника;*
- *исключать или исправлять по письменному требованию одного из родителей (законного представителя) воспитанника его недостоверные или неполные персональные данные, а также данные, обработанные с нарушением требований законодательства Российской Федерации;*
- *ограничивать персональные данные воспитанника ОУ при передаче уполномоченным работникам правоохранительных органов или Учредителю только той информацией, которая необходима для выполнения указанными лицами их функций;*
- *запрашивать информацию о состоянии здоровья воспитанника только у родителей (законных представителей);*
- *обеспечить воспитаннику или одному из его родителей (законному представителю) свободный доступ*

к персональным данным воспитанника, включая право на получение копий любой записи, содержащей его персональные данные;

- *предоставить по требованию одного из родителей (законного представителя) воспитанника полную информацию о его персональных данных и обработке этих данных.*

5.2.Лица, имеющие доступ к персональным данным воспитанника (операторы), не вправе предоставлять персональные данные воспитанника в коммерческих целях.

5.3.При принятии решений, затрагивающих интересы воспитанника, администрации образовательного учреждения запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

VI. Права родителей (законных представителей) в целях обеспечения защиты персональных данных детей

6.1.В целях обеспечения защиты персональных данных, хранящихся в ОУ, родители (законные представители) имеют право на бесплатное получение полной информации:

- *о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;*
- *о перечне обрабатываемых персональных данных и источниках их получения;*
- *о сроках обработки персональных данных;*
- *юридических последствиях обработки их персональных данных.*

6.2.Родители (законные представители) имеют право:

- *на бесплатное получение полной информации о своих персональных данных и обработке этих данных;*
- *на свободный бесплатный доступ к своим персональным данным, в т.ч. на получение копии любой записи, содержащей персональные данные своего ребёнка, за исключением случаев, предусмотренных Федеральным Законом;*
- *требовать исключить или исправить неверные персональные данные, а также данные, обработанные с нарушением требований;*
- *требовать исключить или исправить неверные или неполные персональных данных, а также данных, обработанных с нарушением требований законодательства. При отказе администрации исключить или исправить персональные данные воспитанника родитель (законный представитель) имеет право заявить в письменной форме администрации ОУ о своем несогласии с соответствующим обоснованием такого несогласия;*
- *Персональные данные оценочного характера родитель (законный представитель) имеет право дополнить заявлением, выражающим его собственную точку зрения; требовать извещения заведующим ОУ всех лиц, которым ранее были сообщены неверные или неполные персональные данные воспитанника или родителя (законного представителя), обо всех произведённых в них исключениях, исправлениях или дополнениях;*
- *обжаловать в суде любые неправомерные действия или бездействия заведующего при обработке и защите его персональных данных или своего ребёнка.*

6.3. Родители (законные представители) воспитанников образовательного учреждения не должны отказываться от своих прав на сохранение и защиту тайны.

VII. Обязанности родителей в целях обеспечения достоверности персональных данных

7.1.В целях обеспечения достоверности персональных данных родители (законные представители) воспитанников обязаны:

- *при оформлении представлять достоверные сведения о себе и своем ребенке в порядке и объёме, предусмотренном настоящим Положением, а также законодательством Российской Федерации;*
- *в случае изменения своих персональных данных и своего ребёнка, сообщать об этом заведующему в течение 5 рабочих дней.*

VIII. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

8.1.Защита прав воспитанника и родителя (законного представителя) ребенка, установленных законодательством Российской Федерации и настоящим Положением, осуществляется судом в целях пресечения неправомерного использования персональных данных воспитанника и родителя (законного представителя), восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.

8.2.Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных воспитанника и родителя (законного представителя), привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной

и уголовной ответственности в порядке, установленном федеральными законами.
8.3.Персональная ответственность — одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.
8.4.За нарушение правил хранения и использования персональных данных, повлекшее за собой материальный ущерб образовательного учреждения, работник (оператор) несет материальную ответственность в соответствии с действующим трудовым законодательством.
8.5.Материальный ущерб, нанесенный субъекту персональных данных за счет ненадлежащего хранения и использования персональных данных, подлежит возмещению в порядке, установленном действующим законодательством.
8.6.Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом № 152-ФЗ «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

IX. Заключительные положения

9.1.Настоящее Положение является локальным нормативным актом ОУ, принимается на Общем собрании работников Образовательного учреждения, с учетом мнения родителей (законных представителей) и утверждается (либо вводится в действие) приказом заведующего образовательным учреждением.
9.2.Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации.
9.3.Положение принимается на неопределенный срок.
9.4. Изменения и дополнения к Положению утверждаются (либо вводятся в действие) приказом заведующего образовательным учреждением.
9.5.После принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.

Приложение №1

СОСТАВ И СОДЕРЖАНИЕ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, НЕОБХОДИМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ КАЖДОГО ИЗ УРОВНЕЙ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных	+	+	+	+

	технических средств				
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+

III. Ограничение программной среды (ОПС)

ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				

IV. Защита машинных носителей персональных данных (ЗНИ)

ЗНИ.1	Учет машинных носителей персональных данных			+	+
ЗНИ.2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.7	Контроль подключения машинных носителей персональных данных				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания		+	+	+

V. Регистрация событий безопасности (РСБ)

РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти				
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ.7	Защита информации о событиях безопасности	+	+	+	+

VI. Антивирусная защита (АВЗ)

АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+

VII. Обнаружение вторжений (СОВ)

СОВ.1	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+

VIII. Контроль (анализ) защищенности персональных данных (АНЗ)

АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+

IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)

ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+
ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				

X. Обеспечение доступности персональных данных (ОДТ)

ОДТ.1	Использование отказоустойчивых технических средств				
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+

ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+

XI. Защита среды виртуализации (ЗСВ)

ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+

XII. Защита технических средств (ЗТС)

ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	+	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)

ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+

ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода				
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи				
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю				
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных				
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов				
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+

XIV. Выявление инцидентов и реагирование на них (ИНЦ)

ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+

ИНЦ.5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+

XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)

УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

"+" - мера по обеспечению безопасности персональных данных включена в базовый набор мер для соответствующего уровня защищенности персональных данных.
Меры по обеспечению безопасности персональных данных, не обозначенные знаком "+", применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер по обеспечению безопасности персональных данных.

Приложение № 2

Форма уведомления о получении персональных данных у третьей стороны

Уведомление

Уважаемый_____ _____
(Ф.И.О.)

В связи с_____
(указать причину)

у ГБДОУ детский сад №45 Пушкинского района СПб возникла необходимость получения следующей информации,составляющей Ваши персональные данные_____
_____
(перечислить информацию)

Просим Вас предоставить указанные сведения_____
(кому)

в течение трех рабочих дней с момента получения настоящего уведомления. В случае невозможности предоставить указанные сведения просим в указанный срок дать письменное согласие на получение ГБДОУ детский сад №45 Пушкинского района СПб необходимой информации из следующих источников

_____
(указать источники)

следующими способами:_____
(автоматизированная обработка, иные способы)

По результатам обработки указанной информации ГБДОУ детский сад №45 Пушкинского района СПб планируется принятие следующих решений, которые будут доведены до Вашего сведения

_____
(указать решения и иные юридические последствия обработки информации)

Против принятого решения, Вы, имеете право заявить свои письменные возражения в указанный срок с _____по_____.

Информируем Вас о последствиях Вашего отказа дать письменное согласие на получение ГБДОУ детский сад №45 Пушкинского района СПб указанной информации _____
(перечислить последствия)

Информируем Вас о Вашем праве в любое время отозвать свое письменное согласие на обработку персональных данных.

Настоящее уведомление на руки получил:

«___ »_____20_____ г _____(_____)
(подпись) (Ф.И.О.)

Приложение № 2

Форма заявления – согласия на получение персональных данных у третьей стороны

Заведующему ГБДОУ детским садом №45
Пушкинского района СПб
_____

От_____

проживающего по адресу:
_____
ул._____
дом._____
тел._____

Заявление-согласие на получение персональных данных родителя (законного

представителя) и своего ребёнка у третьей стороны

Я, _____
(ФИО, далее - «Законный представитель»),
действующий(ая) от себя и от имени своего несовершеннолетнего(ей):_____
(ФИО ребенка, дата рождения),

Паспорт _____№ _____ выдан_____«_____ »_____ 20___ г.
_____на получение следующих персональных данных:_____
(согласен / не согласен)
_____

_____
Для обработки в целях_____
_____
_____
У следующих лиц_____

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их получение.

" ____ " _____20 __г. _____ (_____)

(подпись) (ФИО)

Приложение № 3

Государственное бюджетное дошкольное образовательное учреждение
детский сад № 45 Пушкинского района Санкт-Петербурга
196634, Россия, Санкт-Петербург, поселок Шушары, Славянка, Ростовская улица, д. 25 , корп. 1, литера А
телефон/факс (812) 320-40-80, (812) 320-40-81

СОГЛАСИЕ
субъекта на обработку его персональных данных и данных его ребёнка/воспитанника

Я,
_____,
Ф. И. О. родителя (законного представителя)
проживающий (ая) по адресу: _____
паспорт (другой документ, удостоверяющий личность): серия _____ №_____, выдан
«____»_____ _____года
_____,
являясь родителем (законным представителем) ребенка_____
(Ф. И. О.ребенка)
посещающий ГБДОУ детский сад № 45 Пушкинского района СПб(далее-ДОУ), в соответствии с Федеральным Законом от 27.07.2006 №152-ФЗ «О персональных данных», даю согласие на обработку своих персональных данных (Далеее - ПДн) и данных своего ребенка:

фамилия, имя, отчество, пол, дата рождения,
медицинские заключения о состоянии здоровья ребенка,
страховое свидетельство обязательного медицинского страхования,
паспортные данные родителя (законного представителя) и данные свидетельства о рождении,
адрес регистрации, адрес проживания,
домашний или личный телефоны,
статус (если есть), гражданство; родной язык,
данные об образовании,
социальное положение семьи для решения социальных проблем;
дата поступления в образовательное учреждение,
дата и причина отчисления из образовательного учреждения.

С целью обработки и регистрации сведений, необходимых для оказания услуг воспитанникам в области образования в ДОУ, соглашаюсь на обработку персональных данных с использованием средств автоматизации или без использования таких средств, включая хранение этих данных в архивах и размещение в локальной сети ДОУ с целью предоставления доступа к ним. ДОУ вправе рассматривать ПДн в применении к Федеральному Закону «О персональных данных» как общедоступные при следующих условиях: обработка данных осуществляется только в целях уставной деятельности, данные доступны ограниченному кругу лиц.

Для ограничения доступа могут использоваться соответствующие средства, не требующие специальных разрешений и сертификации. Доступ может предоставляться административным и педагогическим работникам только в целях уставной деятельности. Открыто могут публиковаться только фамилии, имена и отчества обучающегося и родителей (законных представителей), в связи с названиями и мероприятиями ДОУ и его структурных подразделений в рамках уставной деятельности, т.ч. на сайтах учреждений системы образования, в целях распространения положительного опыта достижений ребенка.

Я предоставляю ОУ право осуществлять следующие действия (операции) с ПДн: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение.

Я проинформирован(а) и согласен(а) с тем, что информация о ДОУ, организации и содержании воспитательного процесса является общедоступной и может публиковаться в открытых источниках. ДОУ вправе включать обрабатываемые персональные данные обучающегося в списки (реестры) и отчетные формы, предусмотренные нормативными документами федеральных и муниципальных органов управления образованием, регламентирующих предоставление отчетных данных ДОУ. Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес ДОУ по почте заказным письмом с уведомлением о вручении, либо вручен лично под расписку представителю ДОУ.

С Положением о защите персональных данных воспитанников и их родителей (законных представителей) в ДОУ ознакомлен(а), права и обязанности в области защиты персональных данных мне разъяснены.

Согласие действительно с даты заполнения настоящего заявления и до расторжения договора об образовании по образовательном программе между Родителем (законным представителем) и ДОУ.

Адрес оператора персональных данных ДОУ: 196634, Россия, Санкт-Петербург, поселок Шушары, Славянка, Ростовская улица, д. 25 , корп. 1, литера А, Телефон/факс (812) 320-40-80,(812) 320-40-81

Подпись родителя (законных представителей) _____ /_____/ (Ф.И.О.)

Дата заполнения листа согласия «_____»_____20 года

Приложение №4

Форма отзыва согласия на обработку персональных данных своих и своего ребёнка

Заведующему ГБДОУ детским садом №45
Пушкинского района СПб
_____

От_____

проживающего по адресу:
_____
ул._____
дом._____
тел._____

Заявление
отзыв согласия на обработку персональных данных своих
и своего ребёнка

Я,_____
(ФИО, далее - «Законный представитель»),

действующий(ая) от себя и от имени своего несовершеннолетнего(ей):

_____
(ФИО ребенка, дата рождения),

Паспорт №_____серия _____ выдан «_____ »
_____20___г.

прошу Вас прекратить обработку моих персональных данных в связи с
_____
(указать причину)

Ознакомлен(а) с возможными последствиями моего отказа дать письменное согласие на их получение.

« ____ »_____ 20___г.

Приложение №5

Форма расписки о неразглашении персональных данных

Расписка
о неразглашении персональных данных

Я, _____
(Ф.И.О.)
_____, ознакомлен(на) с Положением о защите персональных данных воспитанников и
(должность)

родителей (законных представителей). Заведующему обязуюсь не разглашать сведения, содержащие персональные данные субъектов персональных данных, ставшие мне известными в связи с исполнением мною трудовых (должностных) обязанностей.

Обязуюсь:

– хранить в тайне известные мне конфиденциальные сведения (включая персональные данные),

– информировать руководителя о фактах нарушения порядка обращения с конфиденциальными сведениями, о ставших мне известным попытках несанкционированного доступа к информации;

– соблюдать правила пользования документами, порядок их учета и хранения, обеспечивать в процессе работы сохранность информации, содержащейся в них, от посторонних лиц;

– знакомиться только с теми служебными документами, к которым получен доступ в силу исполнения своих служебных обязанностей.

С перечнем сведений конфиденциального характера, обязанностями о неразглашении данных сведений, ставших известными мне в результате выполнения должностных обязанностей, и ответственностью за разглашение этих сведений ознакомлен(а):

Об ответственности за разглашение указанных сведений предупрежден(на).

"_____ "_____ 20_____ г _____(_____)
(подпись) (Ф.И.О.)