

Принято

Общим собранием трудового
коллектива МБДОУ ЦРР-Д/с №26
«Кустук»
от 28.08.2014г. № 1

Утверждено

Приказом Заведующей
МБДОУ ЦРР-Д/с №26 «Кустук»
от 29.08.2014 г. № 01-09/25

**Положение
о защите персональных данных работников
и доступе к электронным базам данных
Муниципального бюджетного дошкольного образовательного учреждения
«Центр развития ребенка – Детский сад № 26 «Кустук»»
городского округа «город Якутск»**

1. Общие положения

1.1. Настоящее Положение разработано на основе Федерального закона «О персональных данных» от 27.07.2006г. № 152-ФЗ с изменениями и дополнениями, Федерального закона «Об образовании в Российской Федерации» от 29.12.2012 г. №273-ФЗ, Устава Муниципального бюджетного дошкольного образовательного учреждения «Центр развития ребенка - Детский сад №26 «Кустук» городского округа «город Якутск» (далее - Учреждение).

1.2. Настоящее Положение устанавливает порядок учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников Учреждения.

1.3. При разработке настоящего Положения учитываются:

- Конституция РФ от 12.12.1993;
- Трудовой кодекс РФ;
- Кодекс РФ об административных правонарушениях № 195-ФЗ от 30.12.2001 г.;
- Федеральный закон № 24-ФЗ от 20.02.1995 «Об информации, информатизации и защите информации»;

1.4. Основная цель Настоящего положения является разработка комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся в Учреждении, посредством планомерных действий по совершенствованию организации труда.

1.5. Положение о защите персональных данных и изменения к нему утверждаются приказом Заведующей Учреждением. Все работники Учреждения должны быть ознакомлены под расписку с данным Положением и изменениями к нему.

2. Понятие и состав персональных данных

2.1. Под персональными данными работников понимается информация, необходимая Заведующей в связи с трудовыми отношениями и касающаяся конкретного работника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией. К персональным данным относятся:

- все биографические сведения работника;
- образование;
- специальность,
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;

- домашний телефон, номер мобильного телефона;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т-2) и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке педагогических работников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкета;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным работника.

2.2. Данные документы являются конфиденциальными, соответствующий гриф ограничения на них не требуется.

2.3. Информация и документы о персональном составе педагогических работников с указанием их уровня образования, квалификации и опыта работы согласно ч.3. ст.29 №ФЗ-273 подлежат размещению на официальном сайте Учреждения <http://detsad26.yaguo.ru/> и обновлению в течение десяти рабочих дней со дня их получения, изменений после получения письменного согласия работника.

2.4. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

2.5. Собственником информационных ресурсов (персональных данных) — является работник, который заключил трудовой договор с Учреждением и добровольно передал свои персональные данные Заведующей.

2.6. Заведующая Учреждением выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

2.7. Заведующая Учреждением может делегировать заместителям заведующей, старшему воспитателю, делопроизводителю право обработки персональных данных работников для выполнения функциональных обязанностей, которые требуют знания персональных данных работников или связана с обработкой этих данных.

2.8. Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к Заведующей Учреждением за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

3. Принципы создания, обработки и хранения персональных данных

3.1. Обработка персональных данных включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение.

3.2. Получение, хранение, комбинирование, передача или любое другое использование персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении, обеспечения личной безопасности работника,

контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.3. Все персональные данные работника получаются у него самого. Если персональные данные работника, возможно, получить только у третьей стороны, то работник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие.

3.4. Заведующая Учреждением должна сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.5. Не допускается получение и обработка персональных данных работника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях, за исключением случаев, предусмотренных законодательством Российской Федерации.

3.6. Пакет анкетно-биографических и характеризующих материалов (далее «Личное дело») работника формируется в «Личное дело» после издания приказа о его приеме на работу. «Личное дело» обязательно содержит личную карточку формы Т-2, а также может содержать документы, содержащие персональные данные сотрудника, в порядке, отражающем процесс приема на работу: заявление работника о приеме на работу; анкета; характеристика-рекомендация; результат медицинского обследования на предмет годности к осуществлению трудовых обязанностей; копия приказа о приеме на работу; расписка работника об ознакомлении с документами Учреждения, устанавливающими порядок обработки персональных данных работников, а также об его правах и обязанностях в этой области; расписка об ознакомлении его с локальными нормативными актами Учреждения.

3.6. Все документы хранятся в файлах, файлы содержатся в папках в алфавитном порядке фамилий работников.

3.7. Анкета является документом «Личного дела», представляющим собой перечень вопросов о биографических данных работника, его образовании, выполняемой работе с начала трудовой деятельности, семейном положении, месте прописки или проживания и т.п. Анкета заполняется работником самостоятельно при оформлении приема на работу.

3.8. При заполнении анкеты работник должен заполнять все ее графы, на все вопросы давать полные ответы, не допускать исправлений или зачеркивания, прочерков, помарок, в строгом соответствии с записями, которые содержатся в его личных документах.

3.9. В графе «Ближайшие родственники» перечисляются все члены семьи работника с указанием степени родства (отец, мать, муж, жена, сын, дочь, родные брат и сестра); далее перечисляются близкие родственники, проживающие совместно с работником. Указываются фамилия, имя, отчество и дата рождения каждого члена семьи.

При заполнении анкеты и личной карточки Т-2 используются следующие документы:

- паспорт;
- трудовая книжка;
- военный билет;
- документы об образовании.

3.10. «Личное дело» пополняется на протяжении всей трудовой деятельности работника в Учреждении. Изменения, вносимые в карточку Т-2, должны быть подтверждены соответствующими документами.

3.11. Работник, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу документы, проверяет полноту их

заполнения и правильность указываемых сведений в соответствии с предъявленными документами.

3.12. При обработке персональных данных Заведующая Учреждением вправе определять способы обработки, документирования, хранения и защиты персональных данных работников на базе современных информационных технологий.

3.13. Работник имеет право на:

- полную информацию о своих персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных действующим законодательством Российской Федерации;
- доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе Заведующей Учреждением исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия.

4. Доступ к персональным данным работников

4.1. Внешний доступ.

К числу массовых потребителей персональных данных вне Учреждения можно отнести государственные и негосударственные функциональные структуры:

- Учредитель - Округная администрация города Якутска,
- Управление образования Округной администрации города Якутска;
- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды.

4.2. Внутренний доступ.

Внутри Учреждения к разряду потребителей персональных данных относятся работники, которым эти данные необходимы для выполнения должностных обязанностей: все сотрудники бухгалтерии, делопроизводитель, заместители заведующей, старший воспитатель.

4.3. В кабинете Заведующей Учреждением хранятся личные карточки работников, работающих в настоящее время, в специально оборудованном шкафу или сейфе, которые запираются. Личные карточки располагаются в алфавитном порядке.

4.4. После увольнения документы по личному составу передаются на хранение.

5. Передача персональных данных

5.1. Передача персональных данных работника внешнему потребителю:

- Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.
- При передаче персональных данных работника потребителям за пределы Учреждения работодатель не должен сообщать эти данные третьей стороне без

письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных законодательством Российской Федерации.

- Ответы на правомерные письменные запросы других учреждений и организаций даются с разрешения заведующей и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений.

- Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

- Сведения передаются в письменной форме и должны иметь гриф конфиденциальности.

- По возможности персональные данные обезличиваются.

5.2. Передача персональных данных работника **внутреннему потребителю:**

- Заведующая Учреждением вправе разрешать доступ к персональным данным работника только специально уполномоченным лицам.

- Потребители персональных данных должны подписать обязательство о неразглашении персональных данных сотрудников. (Приложение №1)

6. Защита персональных данных

6.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

6.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

6.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Учреждения.

6.3.1. «Внутренняя защита»

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных.

Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами Учреждения. Для защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;

- строгое избирательное и обоснованное распределение документов и информации между работниками;

- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

- знание работниками требований нормативно-методических документов по защите информации и сохранении тайны;

- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками Учреждения;
- воспитательная и разъяснительная работа с работниками по предупреждению утечки ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел работников на рабочие места других сотрудников. Личные дела могут выдаваться на рабочие места только заведующей, заместителем заведующей, старшему воспитателю и в исключительных случаях, по письменному разрешению заведующей другому работнику Учреждения.
- персональные компьютеры, на которых содержатся персональные данные, должны быть защищены паролями доступа.

6.3.2. «Внешняя защита»

Для защиты конфиденциальной информации создаются целенаправленные благоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Учреждения: посетители, сотрудники других учреждений.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в Учреждении.

Для защиты персональных данных работников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим Учреждения;
- порядок охраны территории, зданий, помещений;
- требования к защите информации при интервьюировании и собеседованиях.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

7.1. Персональная ответственность — одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

7.2. Заведующая, разрешающая доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.3. Каждый работник Учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.3. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.

стук»

ения

на «О
ениями,
№273-
ждения
Якутск»

ления и
данным

г.;
зации и

са мер,
ждения,

сдаются
ы быть

кодимая
тника, а
ляющие
вляются
носятся:

Приложение №1

к Положению об обработке и защите персональных данных работников
МБДОУ ЦРР-Д/с № 26 «Кустук» от «29» августа 2014 г.

Обязательство о неразглашении персональных данных сотрудников

стук»

ответственный сотрудник:

бухгалтерия:

ения

на «О
ениями,
№273-
ждения
Якутск»

ления и
данным

г.;
зации и
кса мер,
ждении,
кдаются
ы быть

ходимая
тника, а
ляющие
вляются
носятся: