УТВЕРЖДЕНО:
Заведующий МБДОУ Д/С 4
Кожемяко Я.А.
«__» _____ 2015 г.

СОГЛАСОВАНО:
Председатель ПК МБДОУ Д/С 4
_____
«13» февраля 2015 г.

ПОЛОЖЕНИЕ

о защите персональных данных в МБДОУ Д/С 4

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано на основании ст. 24 Конституции РФ, гл.14 Трудового кодекса РФ, Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информатизации и защите информации» и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».
1.2. Целью Положения является защита персональных данных работников, воспитанников, родителей (законных представителей) воспитанников (далее по тексту «носителей персональных данных») от несанкционированного доступа, неправомерного их использования или утраты.
1.3. Положение определяет порядок работы (получение, обработка, использование, хранение и т.д.) с персональными данными и гарантии конфиденциальности сведений, предоставленных носителями персональных данных в детский сад.
1.4. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.
1.5. Положение утверждается и вводится в действие приказом и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.
1.6. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Персональные данные – информация, необходимая в связи с возникшими правоотношениями, трудового и гражданско-правового характера и касающаяся конкретного работника, воспитанника или родителей (законных представителей) воспитанника. Под информацией понимаются

сведения о фактах, событиях и обстоятельствах жизни конкретного человека, позволяющие идентифицировать его личность.

2.2. В состав персональных данных работника входят:

– паспортные данные;
– анкетные и биографические данные;
– сведения об образовании и специальности;
– сведения о трудовом и общем стаже;
– сведения о составе семьи;
– сведения о воинском учете;
– сведения о социальных льготах;
– наличие судимостей;
– адрес места жительства;
– номер домашнего телефона;
– адрес личной электронной почты;
– место работы или учебы членов семьи и родственников;
– характер взаимоотношений в семье;
– содержание трудового договора;
– состав декларируемых сведений о наличии материальных ценностей;
– результаты медицинских обследований работников на предмет годности к осуществлению трудовых обязанностей.

2.3. К документам, содержащим персональные данные работника, создаваемым в процессе трудовых отношений, относятся:

– трудовой договор 9эффективный контракт);
– основания к приказам по личному составу;
– подлинники и копии приказов по личному составу;
– личное дело;
– трудовая книжка;
– дела, содержащие материалы по повышению квалификации и переподготовке, аттестации, служебным расследованиям;
копии отчетов, направляемые в органы статистики, и др.

2.4. В состав персональных данных воспитанника, родителей (законных представителей) воспитанника входят:

– паспортные данные одного из родителей (законных представителей) воспитанника;
– лицевой счёт одного из родителей (законных представителей) в банке;
– свидетельство о рождении воспитанника;
– сведения о составе семьи;
– сведения о социальных льготах;
– адрес места жительства;
– номер домашнего телефона;
– место работы или учебы членов семьи и родственников;
– характер взаимоотношений в семье;

- содержание договора с родителем (законным представителем) воспитанника;
- результаты медицинских обследований воспитанника.

2.5. К документам, содержащим персональные данные данных воспитанника, родителей (законных представителей) воспитанника создаваемым в процессе возникших правоотношений, относятся:
- договор с родителями (законными представителями) воспитанника ;
- основания к приказам по контингенту воспитанников;
- личное дело воспитанника;
- личное дело воспитанника по компенсационным выплатам;
- сведения о родителях воспитанников;
- медицинская карта и др.

3. ОБЯЗАННОСТИ АДМИНИСТРАЦИИ ОРГАНИЗАЦИИ

3.1. В целях обеспечения прав и свобод человека и гражданина руководитель и его представители при обработке персональных данных обязаны соблюдать следующие общие требования:

3.1.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, обеспечения личной безопасности носителя персональных данных и обеспечения сохранности имущества работодателя.

3.1.2. При определении объема и содержания обрабатываемых персональных данных необходимо руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами.

3.1.3. Все персональные данные следует получать лично у носителя персональных данных. Руководитель должен сообщить о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

3.1.4 Руководитель не имеет права получать и обрабатывать персональные данные о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами правоотношений, данные о частной жизни (информация о жизнедеятельности в сфере семейных, бытовых, личных отношений) могут быть получены и обработаны только с письменного согласия носителя персональных данных.

3.1.5. Руководитель не имеет права получать и обрабатывать персональные данные носителя персональных данных о членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.1.6. При принятии решений, затрагивающих интересы носителя персональных данных, руководитель не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.1.7. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена руководителем за счет средств организации и в порядке, установленном федеральным законом.

4. ПРАВА И ОБЯЗАННОСТИ НОСИТЕЛЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЛАСТИ ЗАЩИТЫ ЛИЧНЫХ ДАННЫХ

4.1. В целях защиты персональных данных, хранящихся у руководителя, носитель персональных данных имеет право:

- получать полную информацию о своих персональных данных и* обработке
этих данных;

-получать свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

-дополнять персональные данные оценочного характера заявлением, выражающим его собственную точку зрения;

-определять представителей для защиты своих персональных данных;

— требовать исключения или исправления неверных или неполных персональных данных;

-требовать извещения всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях и дополнениях;

-обжаловать в суде любые неправомерные действия или бездействия руководителя при обработке и защите его персональных данных;

-на сохранение и защиту своей личной и семейной тайны.

4.2. При отказе руководителя исключить или исправить персональные данные носителя персональных данных они имеют право заявить в письменной форме руководителю о своем несогласии с соответствующим обоснованием такого несогласия.

4.3. Носители персональных данных для сохранения полной и точной информации о них обязаны:

-передавать руководителю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен законами РФ;

-своевременно сообщать руководителю об изменении своих персональных данных.

Носители персональных данных должны быть ознакомлены под роспись с документами организации, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

В целях защиты частной жизни, личной и семейной тайны носитель персональных данных не должен отказываться от своего права на обработку персональных данных только с его согласия, поскольку это может повлечь причинение морального и материального вреда.

5. ПОЛУЧЕНИЕ, ОБРАБОТКА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Получение, обработка, хранение и любое другое использование персональных данных может осуществляться исключительно в целях соблюдения законов и иных нормативных правовых актов.
Персональные данные следует получать у носителя персональных данных лично. Руководитель лично или специально уполномоченное лицо принимает от поступающего на работу, родителя (законного представителя) воспитанника поступающего в детский сад документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с представленными документами. Руководитель должен сообщить работнику, законному представителю воспитанника о целях, предполагаемых источниках и способах получения персональных данных, а также о последствиях отказа дать письменное согласие на их получение.
Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.
Хранение персональных данных должно происходить в порядке, исключающем их утрату или неправомерное использование.

Личное дело и личная карточка носителя персональных данных хранятся в бумажном виде в специально отведенном помещении, обеспечивающем защиту от несанкционированного доступа.
Персональные данные могут также храниться в электронном виде на локальной компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные обеспечивается системой паролей.

6. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

6.1. Внутренний доступ.
6.1.1. Право доступа к персональным данным работника имеют:
руководитель организации;
работник, носитель персональных данных;
работники выполняющие функции кадровой службы;
-работники бухгалтерии (к данным, которые необходимы для выполнения конкретных функций).
6.1.2. Право доступа к персональным данным воспитанника, родителей (законных представителей) воспитанника имеют:
руководитель организации;
должностные лица, назначенные приказом руководителя (к данным, которые необходимы для выполнения должностных обязанностей);
носители персональных данных;
педагогические работники (к данным, которые необходимы для выполнения должностных обязанностей);

-работники бухгалтерии (к данным, которые необходимы для выполнения конкретных функций).

6.1.3. Право получения документов, содержащих персональные данные, непосредственно имеет руководитель организации. По распоряжению руководителя организации сотрудник ответственный за работу с соответствующими документами, обязан лично передать истребуемте документы непосредственно руководителю организации.

6.1.4. Носитель персональных данных имеет право ознакомиться с документами, содержащими его персональные данные, в служебном помещении в присутствии сотрудника ответственного за работу с соответствующими документами.

6.2. Внешний доступ.

6.2.1. К лицам, которым могут быть переданы персональные данные вне организации, при условии соблюдения требований законодательства, относятся:

налоговые инспекции;
правоохранительные органы;
органы статистики;
страховые агентства;
военкоматы;
органы социального страхования;
пенсионные фонды;
подразделения муниципальных органов управления.

6.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

6.2.3. Организации, в которые носитель персональных данных может перечислять денежные средства (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным только при наличии его письменного разрешения.

6.2.4. Сведения о носителе персональных данных могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии заявления носителя персональных данных.

6.2.5. Персональные данные носителя персональных данных могут быть предоставлены родственникам или членам семьи только с письменного разрешения самого носителя персональных данных.

7. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. При передаче персональных данных руководитель., обязан:

- не сообщать персональные данные носителя персональных данных третьей стороне без письменного согласия данного носителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральным законом;

-не сообщать персональные данные в коммерческих целях без его письменного согласия;
-предупредить лиц, получающих персональные данные, 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, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами;
разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
запрашивать информацию о состоянии здоровья носителя персональных данных только в необходимом объеме для выполнения должностных функций;
-передавать персональные данные его представителям в порядке, установленном законодательством РФ, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.
7.2. Копирование и выписка персональных данных разрешаются исключительно в служебных целях и с разрешения руководителя организации.
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.
Сотрудникам, имеющим доступ к персональным данным, запрещается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу.

8. ПОРЯДОК ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. 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.
8.2. 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.

8.3. 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 организации.
Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена работодателем за счет средств организации и в порядке, установленном федеральным законом.
Внутренняя защита.
8.5.1. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать следующие меры:
- 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 работником требований нормативно-методических документов ПО защите информации и сохранению 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 с доступом к базам данных;
организация процесса уничтожения информации;
своевременное выявление нарушения требований разрешительной системы доступа работниками;
воспитательная и разъяснительная работа с сотрудниками, цель которой - предупредить утрату ценных сведений при работе с конфиденциальными документами.
8.5.2. Все файлы, содержащие персональные данные в электронном виде, должны быть защищены паролем.
8.6. Внешняя защита.
8.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладеть персональными данными. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания документа и др.
8.6.2. Распределение функций, рабочие процессы, технология составления, оформления, ведения и хранения документов, содержащих персональные данные, является закрытой от посторонних лиц информацией.

Под посторонним лицом понимается любое лицо, не являющееся работником организации.
Для обеспечения внешней защиты персональных данных необходимо предпринять следующие меры:
-прием, учет и контроль деятельности посетителей должна вести служба безопасности с применением систем видеонаблюдения;
ввести в организации пропускной режим;
посетителей фиксировать в Книге учета посетителей с указанием времени посещения и заинтересованного работника организации.
8.7. Все лица, в должностные обязанности которых входит получение, обработка и защита персональных данных, при приеме на работу обязаны подписать обязательство о неразглашении персональных данных.
8.8. По возможности персональные данные обезличиваются.
9. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ
9.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.
9.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.
9.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.
9.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет личную ответственность за сохранность носителя и конфиденциальность информации.
9.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.
9.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом РФ дисциплинарные взыскания.
9.5.2. Должностные лица, в обязанность которых входит ведение персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов либо несвоевременное предоставление таких документов или

иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях РФ. 9.5.3. Нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения, влечет привлечение виновного к ответственности в соответствии с Уголовным кодексом РФ.

Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

Защита прав граждан, установленных настоящим Положением и законодательством Российской Федерации, осуществляется судом в целях пресечения неправомерного использования персональных данных, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.