

Муниципальное казённое учреждение дополнительного образования
«Детский оздоровительно-образовательный центр» (МКУ ДО «ДООЦ»)

УТВЕРЖДАЮ
Директор МКУ ДО «ДООЦ»
Ю.Ю. Тюрин
Приказ № 20/1 от 28.02.2017 г.



ПОЛОЖЕНИЕ

О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ МКУ ДО «ДООЦ»

г. Бодайбо

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Настоящее Положение разработано на основании ст.24 Конституции Российской Федерации, главы 14 (ст. 85-90) Трудового Кодекса Российской Федерации, Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", Постановления Правительства РФ от 17 ноября 2007 года 3781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
- 1.2. Целью Положения является защита персональных данных работников от несанкционированного доступа, неправомерного их использования или утраты.
- 1.3. Положение определяет порядок работы (получение, обработка, использование, хранение и т.д.) с персональными данными работников и гарантии конфиденциальности сведений, предоставленных работником работодателю.
- 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 директора и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.
- 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. ОСНОВНЫЕ ПОНЯТИЯ

- 2.1. Персональные данные работника – любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями;
- 2.2. Обработка персональных данных – сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных работников Общества;
- 2.3. Конфиденциальность персональных данных – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;
- 2.4. Распространение персональных данных – действия, направленные на передачу персональных данных работников определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным работников каким-либо иным способом;
- 2.5. Использование персональных данных – действия (операции) с персональными данными, совершаемые должностным лицом Общества в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников либо иным образом затрагивающих их права и свободы или права и свободы других лиц;
- 2.6. Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных работников, в том числе их передачи;

- 2.7. Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных работников или в результате которых уничтожаются материальные носители персональных данных работников;
- 2.8. Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику;
- 2.9. Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.
- 2.10. Информация – сведения (сообщения, данные) независимо от формы их представления.
- 2.11. Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

3. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. В состав персональных данных работника входят:

- паспортные данные;
- данные СНИЛС и ИНН
- 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;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных гарантиях;
- номер телефона;
- адрес личной электронной почты;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора;
- результаты медицинских обследований работников на предмет годности к осуществлению трудовых обязанностей.

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

- трудовой договор
- основания к приказам по личному составу;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики.
- сведения о заработной плате сотрудника;
- занимаемая должность;
- справка об отсутствии административного наказания за потребление наркотических средств или психотропных веществ;
- справка об отсутствии судимости.

4. ОБЯЗАННОСТИ РАБОТОДАТЕЛЯ

- 4.1. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:
- 4.1.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативно-правовых актов, содействия работнику в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работника, контроля количества и качества выполняемой работы и обеспечения сохранности имущества работодателя.
 - 4.1.2. При определении объема и содержания обрабатываемых персональных данных работника, работодатель должен руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами.
 - 4.1.3. Работодатель обязан ознакомить под расписку работника и его представителей с документами организации, устанавливающими порядок обработки персональных данных работника, а также об их правах и обязанностях в этой области.
 - 4.1.4. Все персональные данные работника следует получать 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. Работодатель должен сообщить работнику 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.
 - 4.1.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни могут быть получены и обработаны работодателем только с его письменного согласия.
 - 4.1.6. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.
 - 4.1.7. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.
 - 4.1.8. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств и в порядке, установленном федеральным законом.

5. ПОЛУЧЕНИЕ, ОБРАБОТКА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА

- 5.1. Получение, обработка, хранение и любое другое использование персональных данных работника может осуществляться исключительно в целях соблюдения законов и иных нормативно-правовых актов, содействия работнику в трудоустройстве, обучении, продвижении по работе, обеспечения личной безопасности работника, контроля качества выполняемой работы, очередности предоставления ежегодного отпуска, установления размера заработной платы.
- 5.2. Персональные данные следует получать у него самого. Представитель работодателя (специально уполномоченное лицо) принимает от поступающего на работу лица документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с представленными документами. 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. Работодатель должен сообщить работнику о

целях, предполагаемых источниках и способах получения персональных данных, а также о последствиях отказа работника дать письменное согласие на их получение.

- 5.3. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные носители информации.
- 5.4. Хранение персональных данных должно происходить в порядке, исключающем их утрату или неправомерное использование.
- 5.5. Личное дело и личная карточка работника (Т - 2) хранятся в бумажном виде в папках в металлическом, запирающемся шкафу, обеспечивающем от несанкционированного доступа.
- 5.6. Персональные данные работника могут также храниться в электронном виде на локальной компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные работника, обеспечивается системой паролей.

6. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

- 6.1. При передачи персональных данных работника работодатель обязан:
 - не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
 - не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
 - предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;
 - разрешать доступ к персональным данным работника только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
 - запрашивать информацию о состоянии здоровья работника только в объеме, необходимом для определения возможности выполнения работником трудовых функций;
 - передавать персональные данные работника его представителям в порядке, установленном Трудовым кодексом РФ, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций;
- 6.2. Копирование и выписка персональных данных работника разрешаются исключительно в служебных целях по письменному запросу и с разрешения директора.
- 6.3. Передача персональных данных работника от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.
- 6.4. Сотрудникам, имеющим доступ к персональным данным работника, запрещается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу.

7. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

- 7.1. Внутренний доступ (доступ внутри организации).
 - 7.1.1. Право доступа к персональным данным сотрудника имеют:
 - директор организации;
 - заместитель директора по направлению деятельности;
 - работник, ответственный за организацию обработки и хранения персональных данных работника;

- работники бухгалтерии (к данным, которые необходимы для выполнения конкретных функций);
 - сам работник, носитель персональных данных.
- 7.1.2. Право получение документов, содержащих персональные данные работника, непосредственно на рабочее место имеет директор. По распоряжению директора сотрудник кадровой службы, ответственный за работу с соответствующими документами, обязан лично передать истребуемые документы непосредственно директору.
- 7.1.3. Заместители директора имеют право ознакомиться с документами, содержащие персональные данные работника в помещении отдела кадров в присутствии сотрудника ответственного за организацию обработки и хранения персональных данных работника.
- 7.1.4. Работник имеет право ознакомиться с документами, содержащими его персональные данные, в помещении отдела кадров в присутствии сотрудника ответственного за организацию обработки и хранения персональных данных работника.
- 7.2. Внешний доступ.
- 7.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:
- налоговые инспекции;
 - правоохранительные органы;
 - органы статистики;
 - военкоматы;
 - органы социального страхования;
 - пенсионные фонды;
- 7.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.
- 7.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.
- 7.2.4. Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.
- 7.2.5. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

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 компании.
- 8.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

- 8.5. «Внутренняя защита».
- 8.5.1. Для обеспечения внутренней 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 работником 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 подразделения;
 - воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- 8.5.2. Выдача документов на бумажном носителе, содержащих персональные данные работника, на рабочие места заместителей руководителя запрещена.
- 8.5.3. Все файлы, содержащие персональные данные работника в электронном виде, должны быть защищены паролем, который сообщается работнику ответственному за организацию обработки и хранению персональных данных работника.
- 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 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.
- 8.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности компании, посетители, работники других организационных структур.
- 8.6.3. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.
- 8.6.4. Для обеспечения внешней защиты персональных данных сотрудников ведется прием, контроль деятельности посетителей, находящихся в учреждении;
- 8.6.5. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.
- 8.6.6. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

9. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА

- 9.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.
- 9.2. Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

- 9.3. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:
- требовать исключения или исправления не верных или неполных персональных данных.
 - на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
 - дополнять персональные данные;
 - определять своих представителей для защиты своих персональных данных;
 - на сохранение и защиту своей личной и семейной тайны.
- 9.4. Работник обязан:
- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ.
 - своевременно сообщать работодателю об изменении своих персональных данных
- Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов.
- 9.5. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.
- 9.6. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

10. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

- 10.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.
- 10.2. 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.
- 10.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.
- 10.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.
- 10.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.
- 10.5.1. 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 дисциплинарные взыскания.
- 10.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, 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.

- 10.5.3. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.
- 10.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное соби́рание или распространение сведений о частной жизни лица, составляющего 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 наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.
- 10.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.
- 10.7. Защита прав работника, установленных настоящим Положением и законодательством РФ, осуществляется судом в целях пресечения неправомерного использования персональных данных работника, восстановления нарушенных прав и возмещение причиненного ущерба, в том числе морального вреда.