

Муниципальное бюджетное учреждение  
дополнительного образования  
детский оздоровительно-образовательный (профильный)  
центр «Гренада» города Невинномысска

УТВЕРЖДЕНО

Приказом директора

МБУ ДО ДООЦ «Гренада»

№ 55 от 23 октября 2015 г.

\_\_\_\_\_ Кимберг С.В.

« \_\_\_ » \_\_\_\_\_ 20\_\_ г.

**ПОЛОЖЕНИЕ**  
**об обработке и защите персональных данных**  
**муниципального бюджетного**  
**учреждения дополнительного образования**  
**детский оздоровительно-образовательный (профильный)**  
**центр «Гренада» города Невинномысска**

г. Невинномысск  
2015 г.

## I. Общие положения

1.1. Настоящее Положение устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным сотрудников муниципального бюджетного учреждения дополнительного образования детский оздоровительно-образовательный (профильный) центр «Гренада» города Невинномысска (далее учреждение), обучающихся и их родителей (законных представителей), граждан получающих платные услуги, участников семинаров, конкурсов, соревнований, слетов; проводящихся в учреждении, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.

1.2. Положение об обработке и защите персональных данных сотрудников регламентируется Федеральным законом Российской Федерации от 27.06.2006 года № 152-ФЗ «О персональных данных», нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора. Под сотрудниками подразумеваются лица, имеющие трудовые отношения с учреждением. Обучающимися в учреждении считаются лица проходящие обучение по программам дополнительного образования. Участниками семинаров, конкурсов, соревнований и слетов считаются лица прибывающие в Учреждение для участия в соответствующих мероприятиях.

1.3. Настоящее Положение является развитием комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся и обрабатываемых в учреждении.

1.4. Положение об обработке и защите персональных данных и изменения к нему вводятся приказом по общей деятельности учреждения и утверждаются Директором. Все сотрудники учреждения должны быть ознакомлены под расписку с данным Положением и изменениями к нему.

1.5. Под персональными данными сотрудников понимается информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, а также сведения о фактах, событиях и обстоятельствах жизни лица, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией. К персональным данным относятся:

- все биографические сведения сотрудника;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес местожительства;
- домашний телефон;

- 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 Т2) и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, 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, определяемые нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора, Положением об обработке и защите персональных данных и приказами директора учреждения.

Указанные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

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

1.7. Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который стал сотрудником или обучающимся данного учреждения. Субъект персональных данных самостоятельно решает вопрос передачи работодателю своих персональных данных.

1.8. Оператором персональных данных является муниципальное бюджетное учреждение дополнительного образования детский оздоровительно-образовательный (профильный) центр «Гренада» города Невинномысска, которому сотрудник (обучающийся) добровольно передает во владение свои персональные данные. Оператор выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

1.9. Права и обязанности работодателя в трудовых отношениях осуществляются физическим лицом, уполномоченным работодателем. Указанные права и обязанности он может делегировать нижестоящим руководителям – своим заместителям, руководителям структурных подразделений, работа которых требует знания персональных данных работников или связана с обработкой этих данных. Допускается привлекать для обработки персональных данных уполномоченные организации на основе соответствующих договоров и соглашений.

1.10. Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или оператору персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

## II. Принципы обработки персональных данных

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

2.2. Получение, хранение, комбинирование, передача или любое другое использование персональных данных сотрудника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.3. Получение персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособнадзора, настоящим Положением и приказами учреждения на основе согласия субъектов на обработку их персональных данных. Все персональные данные сотрудника получают у него самого. Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Оператор не вправе требовать от субъекта персональных данных предоставления информации о его национальной и расовой принадлежности, политических и религиозных убеждений и о его частной жизни, а также его членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев предусмотренных законодательством.

2.4. Оператор должен сообщить субъекту персональных данных 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.

2.5. Без согласия субъектов осуществляется обработка:

- общедоступных персональных данных или содержащих только фамилии, имена и отчество;
- обращений и запросов организаций и физических лиц;
- регистрация и отправка корреспонденции почтовой связью;
- оформление разовых пропусков;
- обработка персональных данных для исполнения трудовых договоров;
- в иных случаях, предусмотренных законодательством Российской Федерации.

2.6. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ возможно получение и обработка данных о частной жизни сотрудника только с его письменного согласия.

2.7. Пакет анкетно-биографических и характеризующих материалов (далее пакет) субъекта персональных данных формируется после издания приказа о его приеме (зачислении) на работу (обучение). Пакет обязательно содержит личную карточку формы Т-2, а также может содержать документы, содержащие персональные данные сотрудника, в порядке, отражающем процесс приема (зачисления) на работу (обучение).

Все документы хранятся в папках в алфавитном порядке фамилий сотрудников (обучающихся).

Пакет пополняется на протяжении всей трудовой деятельности (обучения) в данном учреждении. Изменения, вносимые в карточку Т-2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

2.8. Сотрудник кадрового отдела, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу сотрудника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами.

2.9. Под блокированием персональных данных понимается временное прекращение операций по их обработке по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

2.10. При обработке персональных данных сотрудников Оператор в лице Директора вправе определять способы обработки, документирования, хранения и защиты персональных данных сотрудников учреждения на базе современных информационных технологий.

2.11. Сотрудник обязан:

- передавать Оператору комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;
- своевременно сообщать об изменении своих персональных данных.

### III. Доступ к персональным данным

3.1. Обработка и использование персональных данных осуществляется в целях, указанных в соглашениях с субъектами персональных данных, а также в случаях, предусмотренных нормативно-правовыми актами Российской Федерации. Не допускается принятие на основании исключительно автоматизированной обработки персональных данных управленческих решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы. В случае увольнения, отчисления субъекта персональных данных и иного достижения целей обработки персональных данных, зафиксированных в письменном соглашении, Оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами. Правила обработки и использования персональных данных устанавливаются отдельными регламентами и инструкциями Оператора.

Персональные данные добровольно передаются субъектом непосредственно держателю этих данных и потребителям внутри учреждения исключительно для обработки и использования в работе.

#### 3.2. Внешний доступ.

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

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

#### 3.3. Внутренний доступ.

Персональные данные могут храниться в бумажном и электронном виде централизованно или в соответствующих структурных подразделениях с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации мер по защите персональных данных. Право на обработку персональных данных предоставляется работникам структурных подразделений и должностным лицам, определенным данным Положением, распорядительными документами и иными письменными указаниями Оператора.

Внутри учреждения к разряду потребителей персональных данных относятся сотрудники функциональных структурных подразделений,

которым эти данные необходимы для выполнения должностных обязанностей:

- ответственный за кадровую работу;
- сотрудники бухгалтерии;
- начальники структурных подразделений.

У ответственного за кадровую работу хранятся личные карточки сотрудников, работающих (обучающихся) в настоящее время. Для этого используются специально оборудованные шкафы или сейфы, которые запираются. Личные карточки располагаются в алфавитном порядке.

После увольнения документы по личному составу передаются на хранение в архив.

#### IV. Передача персональных данных

При передаче персональных данных субъекта Оператор должен соблюдать следующие требования:

##### 4.1. Передача внешнему потребителю:

- передача персональных данных от Оператора внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;
- при передаче персональных данных потребителям (в том числе и в коммерческих целях) за пределы учреждения Оператор не должен сообщать эти данные третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта или в случаях, установленных федеральным законом;
- ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения Директора учреждения 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;
- по возможности персональные данные обезличиваются.

4.2. Передача внутреннему потребителю. Директор учреждения вправе разрешать доступ к персональным данным сотрудников определенным должностным лицам, если это связано с выполнением поставленных им задач. Перечень этих лиц отдается приказом по учреждению и уточняется по мере необходимости.

#### V. Защита персональных данных

5.1. 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.

5.2. 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.

5.3. Защита персональных данных представляет собой жестко регламентированный 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.

#### 5.4. «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 сотрудников необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудниками 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 сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места

только Директору учреждения, и в исключительных случаях, по письменному разрешению Директора учреждения, руководителю структурного подразделения;

- персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

#### 5.5. «Внешняя защита»

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся 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 организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадрового обеспечения и оплаты труда.

Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим учреждения;
- порядок охраны территории, зданий, помещений, транспортных средств.

## VI. Права, обязанности и ответственность субъекта персональных данных и Оператора при обработке персональных данных

6.1. В целях защиты своих персональных данных субъект персональных данных в соответствии с Федеральным Законом Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных» за исключением случаев, предусмотренных данным Федеральным Законом, имеет право:

- на получение сведений об Операторе, о месте его нахождения;
- на полную информацию о своих персональных данных и обработке этих данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных законодательством РФ;
- на определение своих представителей для защиты своих персональных данных;

- на доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;
- требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных;
- требовать об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- на обжалование в суде любых неправомерных действий или бездействия со стороны Оператора при обработке и защите его персональных данных.

#### 6.2. Обязанности Оператора.

Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или заблокировать соответствующие персональные данные по предоставлению субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

В случае выявления неправомерных действий с персональными данными Оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя.

В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва,

если иное не предусмотрено соглашением между Оператором и субъектом персональных данных. Об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных).

6.3. Права Оператора на передачу персональных данных третьим лицам.

Оператор не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации

## VII. 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 является обязательным условием обеспечения эффективности этой системы.

7.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

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

7.4. Оператор, а также должностные лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается в приказе об утверждении Положения и иных приказах на руководителей структурных подразделений и конкретных должностных лиц Оператора, обрабатывающих персональные данные.