Муниципальное бюджетное учреждение дополнительного образования
Центр детского туризма, экологии и творчества имени Р.Р. Лейцингера
(МБУДО ЦДТЭиТ им. Р.Р. Лейцингера)
357500, Ставропольский край, г. Пятигорск, ул. Теплосерная, д. 52. Тел. (8793) 39-18-61, e-mail: centurecotvor@yandex.ru

Утверждено
Директор МБУДО ЦДТЭиТ
им. Р.Р. Лейцингера
А.И. Бойко
Приказ от 02.09.2024г. № 37/2

Положение
о защите конфиденциальной информации
в Муниципальном бюджетном учреждении дополнительного образования Центр детского туризма, экологии и творчества имени Р.Р. Лейцингера

1. Общие положения

1.1. Настоящее Положение о защите конфиденциальной информации в Муниципальном бюджетном учреждении дополнительного образования Центр детского туризма, экологии и творчества имени Р.Р. Лейцингера (далее соответственно – Положение, Учреждение) определяет комплекс организационных и технических мероприятий в части защиты конфиденциальной информации при ее обработке и хранении в Учреждении.

1.2. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 г. N 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 29.07.2004 N 98-ФЗ «О коммерческой тайне», Уставом Учреждения и другими нормативно – правовыми актами Российской Федерации, регулирующими отношения в области информации.

1.3. Настоящее Положение утверждается и вводится в действие приказом руководителя Учреждения и является обязательным для исполнения всеми сотрудникам Учреждения, имеющими доступ к конфиденциальной информации Учреждения.

1.4. Обработка конфиденциальной информации в Учреждении может осуществляться исключительно в целях оказания образовательных услуг надлежащего качества и объёма, выполнения трудовых договоров, и в иных предусмотренных законодательством случаях.

1.5. Лица, допущенные к конфиденциальной информации, должны быть ознакомлены с настоящим Положением под подпись.

2. Термины и определения

Информация - сведения (сообщения, данные) независимо от формы их представления;

информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой

осуществляется с использованием средств вычислительной техники.

электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Конфиденциальная информация – любые сведения, составляющие служебную, коммерческую тайну, включая персональные данные сотрудников и обучающихся.

Обладатель конфиденциальной информации - лицо, которое владеет информацией, составляющей конфиденциальную информацию, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим конфиденциальной информации. Обладателем информации, составляющей конфиденциальную информацию, является образовательное учреждение.

Служебная тайна - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании, и в отношении которой обладателем такой информации введен режим коммерческой тайны. Информация может быть отнесена к служебной тайне в том, случае, если она получена, разработана в процессе осуществления трудовых правоотношений и не влечет (не может повлечь) получения прибыли обладателем такой информации.

Служебную тайну организации составляют любые сведения, в том числе сведения, содержащиеся в служебной переписке, телефонных переговорах, почтовых отправлениях, телеграфных и иных сообщениях, передаваемых по сетям электрической и почтовой связи, которые стали известны работнику организации в связи с исполнением им возложенных на него трудовых обязанностей.

К служебной тайне не относится информация, разглашенная образовательным учреждением самостоятельно или с её согласия, а также иная информация, ограничения доступа к которой не допускаются в соответствии с законодательством РФ.

Персональные данные сотрудника, обучающегося – любая информация, относящаяся к сотруднику, обучающемуся, как субъекту персональных данных, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, сведения о фактах, событиях и обстоятельствах жизни сотрудника, обучающегося, позволяющие идентифицировать его личность.

Доступ к конфиденциальной информации - ознакомление определенных лиц с информацией, составляющей тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача конфиденциальной информации - передача информации, составляющей тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Предоставление информации, составляющей тайну, - передача информации, составляющей тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Разглашение конфиденциальной информации - действие или бездействие, в результате которых информация, составляющая тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной

третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Режим конфиденциальности - организационные, технические и иные меры по защите конфиденциальной информации, принимаемые ее обладателем на основании закона или договора.

3. Информация, являющаяся конфиденциальной, и доступ к ней

3.1. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

3.1.1. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

3.2. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

3.3. К информации, доступ к которой ограничен законодательством (информация ограниченного доступа), относятся: государственная тайна, коммерческая тайна, персональные данные, сведения, связанные с профессиональной деятельностью, служебная тайна. Условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение устанавливаются законодательством Российской Федерации.

3.4. Перечень конфиденциальной информации Учреждения утверждается приказом руководителя (Приложение № 1)

3.5. Режим конфиденциальности снимается в случаях обезличивания или по истечении 25 лет срока хранения конфиденциальной информации, если иное не предусмотрено законодательством РФ.

3.6. Персональные данные относятся к категории конфиденциальной информации. Порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников Учреждения, регулируется Положением об обработке и защите персональных данных работников Учреждения.

В установленном законом порядке субъект персональных данных даёт письменное согласие на обработку своих персональных данных. Работник обязан в установленном законодательством порядке предоставлять Учреждению комплекс достоверных, документированных персональных данных, а также своевременно сообщать об изменении своих персональных данных (ставить Учреждение в известность об изменении фамилии, имени, отчества, даты рождения, смены паспорта, что получает отражение в информационной базе данных, а также в документах содержащих персональные данные).

Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения.

3.7. Общее управление обеспечением режима безопасности сведений, содержащих конфиденциальную информацию, осуществляет руководитель Учреждения.

Координацию организации и защиты персональных данных Учреждения осуществляют заместители руководителя в рамках своей компетенции.

Ответственность за обеспечение безопасности данных в информационных системах

несут уполномоченные на работу с данными системами лица.

Ответственность за обеспечение безопасности данных документированной информации несет секретарь Учреждения.

3.8. Список работников, допущенных к работе с конфиденциальной информацией, утверждается приказом руководителя Учреждения.

3.9. С каждым сотрудником, имеющим доступ к конфиденциальной информации, в том числе к персональным данным, заключается Соглашение о неразглашении данной информации. Соглашение в обязательном порядке включает в себя обязательство о неразглашении конфиденциальной информации, в том числе сведений о персональных данных, а также уведомление об ответственности в случае нарушения требований действующего законодательства в сфере обработки конфиденциальной информации.

4. Порядок обращения конфиденциальной информации.

4.1. Сведения, составляющие конфиденциальную информацию могут быть выражены в письменной, устной и иных формах. Конфиденциальная информация, ставшая известной сотруднику из письменных, устных и иных источников, охраняется равным образом.

Все меры конфиденциальности при сборе, обработке и хранении конфиденциальной информации, в том числе персональных данных, распространяются как на бумажные, так и на электронные (с использованием средств автоматизации и без использования средств автоматизации) носители информации.

4.2. Конфиденциальная информация, ставшая известной сотруднику из устных источников, не должна быть им разглашена. В случае разглашения данной информации сотрудник несёт ответственность в установленном законодательством порядке

4.3. При определении объема и содержания конфиденциальной информации, в том числе персональных данных, сотрудники Учреждения обязаны руководствоваться Конституцией РФ и федеральным законодательством.

4.4. Использование конфиденциальной информации, в том числе персональных данных, возможно только в соответствии с целями, определившими ее получение.

4.5. При передаче конфиденциальной информации за пределы Учреждения сотрудники Учреждения не должны сообщать эти данные третьей стороне, за исключением случаев, установленных федеральным законодательством.

Не допускается отвечать на вопросы, связанные с передачей конфиденциальной информацией, по телефону или факсу.

4.6. В случае необходимости оперативного доведения до заинтересованных лиц сведений, составляющих тайну, руководителем ставится резолюция на самом документе, содержащем служебную или коммерческую тайну. Такое разрешение должно содержать перечень фамилий сотрудников, обязанных ознакомиться с документами или их исполнить, срок исполнения, другие указания, подпись руководителя и дату. Руководитель может при необходимости предусмотреть ограничения в доступе конкретных сотрудников к определенным сведениям.

4.7. Не допускается разглашение сведений, составляющих врачебную тайну, лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, кроме случаев, установленных федеральным законодательством.

4.8. Хранение конфиденциальной информации, в том числе персональных данных, должно происходить в порядке, исключающем ее утрату или неправомерное использование.

5. Защита конфиденциальной информации.

5.1. Основными целями защиты конфиденциальной информации в Учреждении являются:

- предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения работниками;

- предотвращение несанкционированного уничтожения, искажения, подделки, копирования, распространения, блокирования информации в информационных системах, установленных в Учреждении;
- предотвращение утрат, уничтожения или сбоев функционирования носителей информации;
- предотвращение неправомерного или случайного доступа к защищаемой информации; обеспечение полноты, целостности, достоверности защищаемой информации;
- сохранение возможности управления процессом обработки и пользования защищаемой информацией.

5.2. В целях установления режима ограниченного доступа и конфиденциальности сведений в Учреждении администрация, а также специально уполномоченные должностные лица, принимает следующие меры:
- осуществляет разработку локальных нормативных актов и инструкций по обеспечению защиты конфиденциальной информации и регламентации конфиденциального делопроизводства;
- заключает договоры (в том числе трудовые) с условием сохранения и обеспечения конфиденциальности информации;
- обеспечивает ограничение доступа к защищаемой информации, оформляет допуск к такой информации, а также осуществляет учёт лиц, получающих доступ к такой информации;
- организует работу сотрудников с конфиденциальной информацией, в том числе с материальными носителями такой информации;
- организует обучение и проверку знаний по обеспечению режима конфиденциальности информации;
- принимает необходимые технические меры, направленные на ограничение доступа посторонних лиц к защищаемой информации.
- организует уничтожение конфиденциальной информации;
- принимает в установленном порядке меры по приостановлению или прекращению обработки конфиденциальной информации, осуществляемой с нарушением требований законодательства;
- проводит служебные проверки в целях установления виновных лиц, допустивших нарушение законодательства о защите конфиденциальной информации, и последующего привлечения их к дисциплинарной ответственности;
- обеспечивает невозможность несанкционированного доступа к документам, содержащим конфиденциальную информацию;
- обеспечивает хранение конфиденциальной информации в порядке, исключающем их утрату или их неправомерное использование.

5.3. Для получения доступа к защищаемой информации сотруднику необходимо пройти процедуру допуска.

Допуск к конфиденциальной информации включает в себя:
- ознакомление работника с законодательством о защите конфиденциальной информации, об ответственности за его нарушение и с локальными нормативными актами о защите конфиденциальной информации в Учреждении;
- принятие работником на себя обязанности по обеспечению конфиденциальности информации, полученной при осуществлении своей трудовой функции в Учреждении, а также после прекращения трудовых отношений на период действия режима конфиденциальности данной информации;
- оформление Обязательства о неразглашении конфиденциальной информации, в том числе сведений о персональных данных, а также уведомление об ответственности в случае нарушения требований действующего законодательства в сфере обработки конфиденциальной информации;
- прохождение обучения и проверки знаний требований по обеспечению конфиденциальности защищаемой информации.

5.4. Процедура допуска осуществляется руководителем или уполномоченным руководителем лицом до подписания трудового договора директором Учреждения:

- руководитель или уполномоченное лицо знакомит под роспись работника с законодательством о защите конфиденциальной информации, об ответственности за его нарушение и с локальными нормативными актами о защите конфиденциальной информации в Учреждении;
- работник знакомится и подписывает: согласие работника на обработку его персональных данных в соответствии с Положением об обработке и защите персональных данных работников Учреждения, Обязательство о неразглашении конфиденциальной информации (Приложение № 2), расписку об ознакомлении с нормативными правовыми актами в сфере защиты конфиденциальной информации (Приложение № 3);
- после подписания трудового договора работник знакомится с зоной своей ответственности в части конфиденциальности информации.

5.5. Документы, указанные в п. 5.4., хранятся в личном деле сотрудника.

5.6. В трудовые договоры с лицами, принимаемыми на работу, связанную с получением, обработкой, хранением, передачей и использованием информации ограниченного доступа, включается условие об обеспечении конфиденциальности таких сведений.

5.7. Работники Учреждения, получившие доступ к конфиденциальной информации, обязуются обеспечивать защиту такой информации.

5.7.1. Обязанности работника по обеспечению конфиденциальности оформляются соответствующим обязательством в рамках Соглашения о неразглашении конфиденциальной информации. В целях обеспечения конфиденциальной информации, работник обязан:
- знать и соблюдать требования по получению, обработке, передаче, хранению, конфиденциальной информации, предусмотренные нормативными правовыми актами, соглашениями, должностной инструкцией, локальными нормативными актами о защите конфиденциальной информации в Учреждении и трудовым договором;
- знать, какие конкретно сведения подлежат защите, а также строго соблюдать правила пользования ими; принимать меры по установлению и сохранению режима конфиденциальности, предусмотренные нормативными правовыми актами о защите конфиденциальной информации в Учреждении;
- работать только с теми конфиденциальными сведениями и документами, к которым он получил доступ в силу своих служебных обязанностей;
- не использовать конфиденциальную информацию ограниченного доступа, ставшую ему известной из письменных, электронных, устных и иных источников, в целях, не связанных с осуществлением трудовой функции;
- не допускать передачу конфиденциальной информации по телефону или факсу;.
- не разглашать конфиденциальную информацию, а также не совершать деяний, влекущих уничтожение или утрату такой информации;
- обеспечить невозможность утраты (целостность и сохранность, соблюдение порядка хранения) документов, содержащих указанные сведения; обеспечить невозможность несанкционированного доступа к документам, содержащим конфиденциальную информацию, находящимся в его ведении;
- незамедлительно сообщать об утрате или несанкционированном уничтожении конфиденциальной информации своему непосредственному руководителю, а также об иных обстоятельствах, создающих угрозу сохранения конфиденциальности такой информации.

5.7.2. При прекращении трудовых отношений с Учреждением работник обязан сдать все материальные носители защищаемой информации, а также ключи от помещений и шкафов, в которых они хранятся, непосредственному руководителю структурного подразделения, из которого он увольняется. Непосредственный руководитель обязан в трехдневный срок передать полученное руководителю Учреждения.

5.8. По факту разглашения конфиденциальной информации, потери документов и иного несанкционированного доступа к конфиденциальным сведениям, проводится служебное расследование, по результатам которого виновные лица привлекаются к ответственности.

5.9. При участии в работе сторонних организаций сотрудник может знакомить их представителей со сведениями, составляющими служебную или коммерческую тайну, только

с письменного разрешения руководителя. Руководитель при этом должен определить конкретные вопросы, подлежащие рассмотрению, и указать, кому и в каком объеме может быть сообщена информация, подлежащая защите.

5.10. По общему правилу доступ посторонних лиц к сведениям, составляющим врачебную тайну, не допускается, за исключением случаев, установленных действующим законодательством, а также настоящим Положением.

5.11. Защита конфиденциальной информации, в том числе персональных данных, представляет собой технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности информации, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Учреждения.

5.12. Защита конфиденциальной информации, в том числе персональных данных, от неправомерного использования или утраты должна быть обеспечена в порядке, установленном действующим законодательством.

Защита включает в себя следующие меры:

- ограничение и регламентация доступа сотрудников к персональным данным с установлением конкретных прав доступа;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками организации;
- рациональное и эргономичное размещение рабочих мест сотрудников организации, имеющих доступ к персональным данным, при котором исключалась бы случайная утечка защищаемой информации;
- ознакомление сотрудников организации с требованиями нормативно – методических документов по защите информации о персональных данных;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации, содержащей персональные данные сотрудников;
- регламентация обращения документов, содержащих персональные данные, на рабочих местах сотрудников организации;
- привлечение к дисциплинарной ответственности лиц, виновных в нарушении законодательства о персональных данных.

6. Требования по получению, обработке, хранению и использованию конфиденциальной информации

6.1. Обработка и хранение конфиденциальной информации осуществляется в таком порядке и таким способом, которые исключают возможность доступа к ней неуполномоченных лиц.

6.2. Не допускается передача и выдача документов, содержащих сведения конфиденциального характера неуполномоченным лицам без законных на то оснований.

6.3. Использование конфиденциальной информации допускается только в служебных целях.

6.4. Хранение конфиденциальной информации осуществляется в порядке, исключающем ее утрату, неправомерное использование или получение доступа неуполномоченными лицами.

6.5. Все документы, содержащие сведения конфиденциального характера должны храниться в сейфах, шкафах, оборудованных замками либо запирающихся за замок помещениях.

6.6. Обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта

персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

7. Организация конфиденциального делопроизводства

7.1. Сведения, составляющие конфиденциальную информацию могут быть выражены в письменной, устной и электронной формах. Конфиденциальная информация, ставшая известной работнику из письменных, устных и электронных источников, охраняется равным образом.

7.2. Все документы, содержащие конфиденциальную информацию, должны сохраняться в режиме конфиденциальности и быть доступными только тем лицам, которые имеют допуск к такой информации в силу исполнения ими своих должностных обязанностей.

7.3. Организация конфиденциального делопроизводства должна исключать ознакомление с информацией иных лиц, не имеющих такого доступа.

7.4. Приказом директора назначаются уполномоченные лица, ответственные за учет, хранение и использование конфиденциальной информации в рамках свой компетенции.

7.5. Контроль за порядком допуска и работы с конфиденциальной информацией осуществляет руководитель структурного подразделения, в котором осуществляется работа и хранение информации, относящейся к конфиденциальной.

При осуществлении контроля лицо, указанное в п. 7.5 настоящего Положения, проверяет: ведение журналов учета при работе с конфиденциальной информацией; состояние помещения, предназначенного для работы с конфиденциальной информацией и ее хранения; наличие носителей конфиденциальной информации.

7.8. В случае необходимости оперативного доведения до заинтересованных лиц сведений конфиденциального характера руководитель может предусмотреть изменения в списке лиц, имеющих доступ к конфиденциальной информации, в том числе доступе конкретных работников к определенным сведениям.

7.9. При работе с документами, содержащими сведения конфиденциального характера, запрещено:

- делать выписки в целях, не связанных с осуществлением трудовой функции;
- знакомить с такими документами, в том числе в электронном виде, других лиц, не имеющих соответствующего доступа;
- использовать информацию из таких документов в открытых сообщениях, докладах, переписке, рекламных изданиях (такое использование допускается только при условии обезличивания информации);
- оставлять на рабочем месте документы и иные носители конфиденциальной информации;
- допускать к компьютерам, содержащим конфиденциальную информацию, посторонних лиц, оставлять включенными компьютеры, содержащие конфиденциальную информацию.

7.10. Передача документов, содержащих конфиденциальную информацию, неуполномоченным лицам допускается, если обработка необходима:

- для исполнения гражданско-правового договора и в соответствии с условиями договора;
- для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица;
- для защиты жизни или жизненно важных интересов гражданина;
- для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы граждан;
- в интересах гражданина и с его письменного согласия.
- для иных целей, предусмотренных законодательством РФ.

7.11. Уничтожение документов, содержащих конфиденциальную информацию осуществляется в следующими способами: сжигание, плавление, шредирование, химическая

обработка. В каждом случае уничтожения составляется акт.

7.12. Проверка соблюдения требований настоящего Положения осуществляется в соответствии с Положением о внутреннем контроле в Учреждении.

8. Ответственность за нарушение режима конфиденциальности.

8.1. Каждый сотрудник Учреждения, получающий для работы документ или иной носитель, содержащий конфиденциальную информацию, несет ответственность за сохранность носителя и конфиденциальность информации.

8.2. К способам нарушения режима конфиденциальности относятся:

- разглашение конфиденциальной информации, обладание которыми входит в круг служебных обязанностей сотрудника, другим сотрудникам, у которых в силу своего служебного положения нет к ним доступа, а также третьим лицам, не являющимся сотрудниками Учреждения;
- разглашение сведений, которые были получены случайным образом, сотрудникам, не имеющим доступа к данной информации, а также третьим лицам, не являющимся сотрудниками Учреждения;
- неправомерное использование конфиденциальной информации;
- утрата документов и иных материальных носителей, содержащих сведения конфиденциального характера;
- неправомерное уничтожение документов, содержащих сведения конфиденциального характера;
- нарушение требований хранения документов, содержащих сведения конфиденциального характера;
- получение информации, составляющей коммерческую тайну, с использованием специальных средств или путем противоправных действий;
- другие нарушения требований законодательства и настоящего Положения.

8.3. За разглашение конфиденциальной информации, а также за нарушение порядка обращения с документами, содержащими сведения конфиденциального характера, работник организации несут предусмотренную законодательством Российской Федерации ответственность и может быть привлечен к дисциплинарной, административной, гражданско-правовой или уголовной ответственности.

Приложение № 1
к Положению о защите конфиденциальной информации
в Муниципальном бюджетном учреждении
дополнительного образования Центр детского туризма,
экологии и творчества имени Р. Р. Лейцингера

Перечень конфиденциальной информации
Муниципального бюджетного учреждения дополнительного образования Центр детского туризма, экологии и творчества имени Р.Р. Лейцингера

В настоящем Перечне предусматриваются категории сведений, представляющих конфиденциальную информацию (персональные данные) (название учреждения), разглашение которых может нанести материальный, моральный или иной ущерб интересам (название учреждения).

Конкретные исполнители и руководитель учреждения несут персональную ответственность за правильность определения сведений, составляющих персональные данные. При этом они должны руководствоваться Указом Президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера».

К конфиденциальной информации Муниципального бюджетного учреждения дополнительного образования Центр детского туризма, экологии и творчества имени Р.Р.Лейцингера (далее – Учреждение) относятся следующие сведения и документы:

№ п/п	Перечень сведений	Срок действия режима конфиденциальности
1.	Учреждение	
1.1.	Сведения о применяемых методах управления в Учреждении	Постоянно
1.2.	Сведения о подготовке, принятии и исполнении решений руководителя по организационным, коммерческим, производственным, научно-техническим и иным вопросам	Постоянно
1.3.	Сведения о планах расширения или сокращения реализации различных видов образовательных услуг и продукции, оказания услуг, выполнения работ и их технико-экономических обоснованиях	Постоянно
1.4.	Сведения о планируемых и заключенных контрактах, договорах, соглашениях о сетевом взаимодействии и взаимном сотрудничестве; информация о подготовке и проведении переговоров с деловыми партнерами Учреждения	Постоянно
1.5.	Сведения, условия конфиденциальности которых установлены в договорах, контрактах, соглашениях и других обязательствах	Постоянно
2.	Финансы	
2.1	Сведения о бухгалтерской, налоговой и управленческой отчетности, о движении средств, о финансовых операциях, о состоянии банковских счетов и производимых операциях, сведения о долговых обязательствах (за исключением годового баланса)	3 года
2.2	Первичные регистры бухгалтерского, налогового и управленческого учета	3 года
2.3.	Информация о финансово-хозяйственной деятельности Учреждения (кроме Плана финансово-хозяйственной деятельности Учреждения	3 года
2.4	Сведения о величине доходов и расходов, о долговых обязательствах, состоянии дебиторской и кредиторской задолженностей (за	3 года

	исключением годового баланса).	
2.5	Сведения, содержащиеся в финансово – договорных схемах Учреждения	+1 год после окончания действия договора
2.6.	Сведения о заработной плате и премировании сотрудников Учреждения	постоянно
3.	Личная безопасность сотрудников	
3.1	Персональные данные, сведения о фактах, событиях и обстоятельствах частной жизни сотрудника.	Постоянно
3.2.	Данные, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством	Постоянно
3.3	Сведения об используемой в коллективе системе стимулов, укрепляющих дисциплину, повышающих производительность труда.	На период действия
3.4.	Сведения о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении; Сведения о временной нетрудоспособности. Сведения об инвалидности, о наличии хронических заболеваний и пр.	постоянно
3.5.	Информация о личных отношениях специалистов как между собой, так и с руководством, сведения о возможных противоречиях, конфликтах внутри коллектива.	3 года
4.	Персональные данные об обучающихся	
4.1.	Персональные данные обучающегося.	Постоянно
4.2.	Персональные данные родителей (законных представителей).	Постоянно
4.3.	Сведения, необходимые для предоставления обучающемуся гарантий и компенсаций, установленных действующим законодательством (в том числе категория семьи для оказания материальной и других видов помощи и сбора отчетности по социальному статусу контингента)	Постоянно
4.4.	Сведения о попечительстве, опеке, отношении к группе социально незащищенных обучающихся; документы (сведения), подтверждающие право на льготы, дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т. п.)	Постоянно
5.	Персональные данные о детях, оставшихся без попечения родителей	
5.1.	Персональные данные детей, оставшихся без попечения родителей.	Постоянно
5.2.	Персональные данные кандидатов в усыновители, приемных родителей, опекунов.	Постоянно
6.	Безопасность	
6.1.	Сведения об охране Учреждения, пропускном и внутриобъектовом режиме, системе сигнализации, о наличии средств контроля и управления доступом.	постоянно
6.2.	Сведения о планах по проведению антитеррористических мероприятий и мероприятий противопожарной безопасности, гражданской обороны	постоянно
6.3.	Сведения о порядке и состоянии защиты конфиденциальной информации, о мерах по совершенствованию системы защиты конфиденциальной информации	постоянно
6.4.	Сведения о защищаемых информационных ресурсах в локальных сетях Учреждения	постоянно
6.5.	Сведения о применяемых методах и средствах защиты помещений, техники, сетей, другого оборудования от утечки защищаемой информации, несанкционированного воздействия на защищаемую информацию	постоянно

6.6.	Сведения о результатах проверок состояния защиты информации, о потенциальных каналах утечки информации; отчетность, содержащая анализ состояния организационно-технических средств защиты информации	постоянно
6.7.	Сведения об установленных программных средствах, автоматизированных системах управления, системах связи и передачи данных, о компьютерном оборудовании осуществляющих прием, обработку, хранение и передачу информации с ограниченным доступом;	постоянно
6.8.	Сведения об используемых сетевых адресах и паролях автоматизированных систем Сведения о паролях, ключах, электронных цифровых подписях	постоянно
6.9.	Содержание базы данных и программного обеспечения автоматизированных систем	постоянно
6.10	Данные о лицах, получивших доступ к конфиденциальной информации	постоянно

Приложение № 2
к Положению о защите конфиденциальной информации
в Муниципальном бюджетном учреждении
дополнительного образования Центр детского туризма,
экологии и творчества имени Р. Р. Лейцингера

Обязательство
о неразглашении конфиденциальной информации
Муниципального бюджетного учреждения дополнительного образования Центр детского туризма, экологии и творчества имени Р.Р. Лейцингера

Я, _____,
(ФИО)
_____,
(должность)
в период трудовых отношений с Муниципальным бюджетным учреждением дополнительного образования Центр детского туризма, экологии и творчества имени Р.Р. Лейцингера (далее – Учреждение) и в течение трех лет после их прекращения обязуюсь:

1. Не разглашать сведения, составляющие конфиденциальную информацию в Учреждении, которые мне будут доверены или станут известны по работе.
2. Не передавать третьим лицам и не раскрывать публично сведения, составляющие конфиденциальную информацию об Учреждении.
3. Выполнять требования Приказов, инструкций и положений по обеспечению сохранности конфиденциальной информацию об Учреждении.
4. В случае попытки посторонних лиц получить от меня конфиденциальную информацию об Учреждении сообщить об этом факте непосредственному руководителю.
5. Сохранять конфиденциальную информацию тех юридических и физических лиц, с которыми у Учреждения имелись/имеются деловые отношения.
6. Не использовать знание конфиденциальной информации Учреждения для занятий любой деятельностью, которая может нанести ущерб Центру, за исключением случаев, установленных законодательством РФ.
7. В случае моего увольнения все носители конфиденциальной информации Учреждения (рукописи, черновики, машинные носители, распечатки на принтерах, изделия и пр.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в Учреждении передать непосредственному руководителю.
8. Об утрате или недостаче носителей конфиденциальной информации, ключей, специальных пропусков, удостоверений от режимных помещений, хранилищ, сейфов, архивов, личных печатей, которые могут привести к разглашению конфиденциальной информации Учреждения, а также о причинах и условиях возможной утечки сведений немедленно сообщать непосредственному руководителю.

Я предупрежден(а), что в случае невыполнения любого из вышеуказанных пунктов настоящего Обязательства, ко мне могут быть применены меры дисциплинарного взыскания в соответствии с трудовым законодательством РФ.

Я ознакомлен (а) с законодательством о защите конфиденциальной информации и с локальными нормативными актами о защите конфиденциальной информации в Учреждении.

Мне известно, что нарушение требований по обеспечению сохранности конфиденциальной информации Учреждения может повлечь уголовную, административную, гражданско-правовую или иную ответственность в соответствии с законодательством Российской Федерации, в виде лишения свободы, денежного штрафа, обязанности по возмещению ущерба Учреждению (убытков, упущенной выгоды) и других наказаний.

«____»_____ 20___г. _____ _____
(подпись) (расшифровка подписи)

Приложение № 3
к Положению о защите конфиденциальной информации
в Муниципальном бюджетном учреждении
дополнительного образования Центр детского туризма,
экологии и творчества имени Р. Р. Лейцингера

Форма расписки об ознакомлении с нормативными правовыми актами в сфере защиты конфиденциальной информации

РАСПИСКА

я _____
(Ф.И.О. работника)
_____
(структурное подразделение, должность).

ознакомлен с:

- Федеральным законом от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Положением о защите конфиденциальной информации в Муниципальном бюджетном учреждении дополнительного образования Центр детского туризма, экологии и творчества имени Р.Р. Лейцингера, утвержденного;

Права и обязанности в области защиты конфиденциальной информации и защиты персональных данных мне разъяснены.

«___»_____20___г. _____ _____
(подпись) (расшифровка подписи)