«УТВЕРЖДАЮ»
Директор МКУ «Центр МИТО»
ЗАТО Видяево
_____ Н.В. Коренкова
«__» _____ 2024 г.

ПОЛОЖЕНИЕ
Об обработке и защите персональных данных

1.Общие положения

1.1.Настоящее Положение об обработке и защите персональных данных **Муниципального казенного учреждения образования «Центр методического и информационно-технического обслуживания» ЗАТО Видяево** (далее - Учреждение) устанавливает порядок получения, учета, обработки, накопления, хранения и защите документов, содержащих сведения, отнесенные к персональным данным работников Учреждения, иных физических лиц.
1.2.Целью настоящего Положения является защита персональных данных работников Учреждения, **иных физических лиц** от несанкционированного доступа и разглашения, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.
1.3.Основанием для разработки настоящего Положения являются Конституция Российской Федерации, Трудовой кодекс Российской Федерации, Федеральные законы от 27.07.2006 № 152-ФЗ «О персональных данных» от 27.07.2006г.,в ред. Федерального закона от 14.07.2022 №266-ФЗ),№ 149-ФЗ «Об информатизации, информационных технологиях и о защите информации», другие действующие нормативные правовые акты РФ.
1.4.Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.
1.5.Режим конфиденциальности персональных данных снимается:
-в случае их обезличивания;
-по истечении 75 лет срока их хранения;
-в других случаях, предусмотренных федеральными законами.
1.6.Настоящее Положение и изменения к нему утверждаются приказом руководителя Учреждения. Все работники Учреждения должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

2.Основные понятия и состав персональных данных

2.1.Для целей настоящего Положения используются следующие основные понятия:

-персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, физическому лицу (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 о физическом лице или о работнике, необходимая работодателю в связи с трудовыми отношениями;

-обработка персональных данных — сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных работников, иных физических лиц;

-конфиденциальность персональных данных — обязательное для соблюдения назначенных ответственных лиц, получивших доступ к персональным данным работников, иных физических лиц, требование не допускать их распространения без согласия работника, иного физического лица или иного законного основания;

-распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

-использование персональных данных — действия (операции) с персональными данными, совершаемые должностными лицами Учреждения в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников, иных физических лиц либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

-блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

-уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

-обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику или физическому лицу;

-общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствие с федеральными законами не распространяется требование соблюдения конфиденциальности;

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

-документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2.Состав персональных данных работника и иных физических лиц, не подлежащих разглашению:
-анкета;
-автобиография;
-образование;
-сведения о трудовом и общем стаже;
-сведения о предыдущем месте работы;
-сведения о составе семьи;
-паспортные данные;
-сведения о воинском учете;
-сведения о заработной плате;
-сведения о поощрениях и взысканиях;
-сведения о социальных льготах;
-занимаемая (замещаемая) должность;
-наличие судимостей;
-адрес места жительства;
-номер домашнего или мобильного телефона;
-содержание трудового или иного договора гражданско-правового характера;
-копии отчетов, направляемые в органы статистики, иные органы государственной власти или местного самоуправления;
-результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей или приеме в Учреждение;
-фотографии и иные сведения, относящиеся к персональным данным.
2.3.Информация, представляемая работником при поступлении на работу в Учреждение, должна иметь документальную форму.
2.4.При заключении трудового договора в соответствии со ст. 65 ТК РФ лицо, поступающее на работу, предъявляет:
-паспорт или иной документ, удостоверяющий личность;
-трудовую книжку, за исключением случаев, когда договор заключается впервые, или работник поступает на работу на условиях совместительства, или трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
-страховое свидетельство государственного пенсионного страхования;
-документы воинского учета для лиц, подлежащих воинскому учету;
-документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;
-свидетельство о присвоении ИНН (при его наличии у работника).
2.5.При оформлении работника кадровой службой заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника.

2.6.В кадровой службе Учреждения создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:
2.6.1.Документы, содержащие персональные данные работников:
-комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;
-комплекс материалов по анкетированию, тестированию, проведению собеседований с кандидатом на должность;
-подлинники и копии приказов (распоряжений) по кадрам;
-личные дела и трудовые книжки;
-дела, содержащие основания к приказу по личному составу;
-дела, содержащие материалы аттестаций работников;
-дела, содержащие материалы внутренних расследований;
-справочно-информационный банк данных по персоналу (картотеки, журналы);
-подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководителю Учреждения;
-копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.
2.7.Документация по организации работы Учреждения:
-должностные инструкции работников;
-приказы, распоряжения, указания руководителя Учреждения;
-документы планирования, учета, анализа и отчетности по вопросам кадровой работы.

3.Сбор и обработка персональных данных

3.1. Сбор и обработка персональных данных работника.
Все персональные данные следует получать непосредственное от работника. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом не менее чем за три рабочих дня и от него должно быть получено письменное согласие (либо письменный отказ), которое работник должен дать в течение пяти рабочих дней с момента получения от работодателя соответствующего уведомления.
В письменном уведомлении работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.
Согласие работника оформляется в письменной форме в двух экземплярах: один из которых предоставляется работнику, второй хранится в учреждении (Приложение №1).
3.1.2.Работник предоставляет работодателю достоверные сведения о себе. Работодатель проверяет достоверность сведений, сверяя данные,

предоставленные работником, с имеющимися у работника документами. Предоставление работником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

3.1.3.Своевременно, в разумный срок, не превышающий 5 рабочих дней, работник обязан лично либо через своего законного представителя сообщать работнику, ответственному за сбор информации, об изменении своих персональных данных либо представить соответствующие документы.

3.1.4.Работник, ответственный за сбор информации, при получении персональных данных или получении измененных персональных данных работника должен:

-проверить достоверность сведений, сверяя данные, представленные работником, с имеющимися у работника документами;

-сделать копии представленных документов;

-подшить в личное дело работника;

-внести соответствующие изменения в кадровые документы;

-при необходимости подготовить и подписать соответствующие документы, в которых отразить соответствующие изменения;

-донести до сведения работников, ответственных за обработку персональных данных, об изменениях этих данных.

3.1.5.Обработка персональных данных работников работодателем возможна только с их согласия либо без их согласия в следующих случаях:

-персональные данные являются общедоступными;

-персональные данные относятся к состоянию здоровья работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;

-по требованию полномочных государственных органов в случаях, предусмотренных Федеральными законами.

3.1.6.Работодатель вправе обрабатывать персональные данные работников только с их письменного согласия.

3.1.7.Форма заявления о согласии работника на обработку персональных данных (Приложение №2) является неотъемлемой частью трудового договора **(контракта), заключаемого с работником.**

3.1.8.Согласие работника не требуется в следующих случаях:

-обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

-обработка персональных данных осуществляется в целях исполнения трудового договора;

-обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

-обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

3.2.Сбор и обработка персональных данных иных физических лиц (субъект персональных данных).

3.2.1.Все персональные данные следует получать непосредственно от субъекта персональных данных. Субъект самостоятельно принимает решение о предоставление своих персональных данных и дает письменное согласие на их обработку Учреждением (Приложение №3).

3.2.2.Письменное согласие не требуется, если обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных.

3.2.3.Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

3.2.4.В случаях,когда Учреждение может получить необходимые персональные данные субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. В уведомлении Учреждение обязано сообщить о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа субъекта дать письменное согласие на их получение. Согласие оформляется в письменной форме в двух экземплярах: один из которых предоставляется субъекту, второй хранится в учреждении (Приложение №4).

3.2.5.Запрещается получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни.

3.2.6.Запрещается получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.2.7.В соответствии со ст. 86 ТК РФ в целях обеспечения прав и свобод человека и гражданина руководитель Учреждения и его законные, полномочные представители при обработке персональных данных работника или иного физического лица должны выполнять следующие общие требования:

3.3.Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов или иных правовых актов, содействия работникам, субъектам персональных данных в трудоустройстве, обучении и профессиональном продвижении, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.3.1.При определении объема и содержания обрабатываемых персональных данных Учреждение должно руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами.

3.3.2.При принятии решений, затрагивающих интересы работника, иного физического лица ответственные должностные лица не имеют права

основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.
3.3.3.Защита персональных данных от неправомерного их использования, утраты обеспечивается Учреждением за счет его средств в порядке, установленном Федеральным законом.
3.3.4.Работники и субъекты персональных данных должны быть ознакомлены под расписку с документами Учреждения, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.
3.3.5.Во всех случаях отказ работника, субъекта персональных данных от своих прав на сохранение и защиту тайны недействителен.

4.Передача и хранение персональных данных

4.1.При передаче персональных данных должностные лица Учреждения должны соблюдать следующие требования:
4.1.2.Не сообщать персональные данные работника и иного физического лица третьей стороне без письменного согласия (Приложения №4), за исключением случаев, когда это необходимо в целях предупреждения угрозы их жизни и здоровью, а также в случаях, установленных федеральным законом.
4.1.3.Предупредить лиц, получивших 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, получившие персональные данные, обязаны соблюдать режим конфиденциальности.
4.1.4.Осуществлять передачу персональных данных в пределах Учреждения в соответствии с настоящим Положением.
4.1.5.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 конкретной функции.
4.1.6.Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.
4.1.7.Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функции.
4.2.Хранение и использование персональных данных:
4.2.1.Персональные данные работников обрабатываются и хранятся в кадровой службе и бухгалтерии Учреждения. Персональные данные иных физических лиц обрабатываются и хранятся в подразделениях Учреждения в соответствии с приказом руководителя.
4.2.2.Персональные данные работников могут быть получены, проходить

дальнейшую обработку и передаваться на хранение, на бумажных и электронных носителях с ограниченным доступом.

4.3.Персональные данные на бумажных носителях хранятся в сейфе.

Персональные данные на электронных носителях защищены паролем доступа, доступ к специализированной программе осуществляется только через личный доступ - пароль, право на использование персональных данных имеют только работники, ответственные за обработку персональных данных.

4.3.1.Личные дела хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Все документы, поступающие в личное дело, располагаются в хронологическом порядке. Личные дела хранятся в специально отведенной секции сейфа, обеспечивающего защиту от несанкционированного доступа.

4.3.2.При получении персональных данных не от работника (за исключением случаев, если персональные данные были предоставлены работодателю на основании Федерального закона или если персональные данные являются общедоступными) или иного физического лица работодатель или уполномоченное им должностное лицо до начала обработки таких персональных данных обязан предоставить работнику или иному физическому лицу следующую информацию:

-наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

-цель обработки персональных данных и ее правовое основание;

-предполагаемые пользователи персональных данных;

-установленные Федеральным законом права субъекта персональных данных.

5.Доступ к персональным данным работников

5.1.Внутренний доступ (доступ внутри Учреждения):

-руководитель Учреждения;

-заместитель руководителя;

-работник кадровой службы;

-руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников своего подразделения);при переводе из одного структурного подразделения в другое доступ к персональным, данным работника может иметь руководитель нового подразделения;

-работники бухгалтерии - к тем данным, которые необходимы для выполнения конкретных функций;

-делопроизводитель, документовед (информация о фактическом месте проживания и контактные телефоны работников);

-непосредственные руководители по направлению деятельности (доступ к персональным данным сотрудников, непосредственно находящихся в его подчинении);

-сам работник, носитель данных;

-сам субъект, носитель данных.

5.1.2.Должностные лица, работники Учреждения, физические лица указанные п.5.1, настоящего Положения, имеют право получать только те персональные данные, которые необходимы им для выполнения своих должностных обязанностей.

5.2.Внешний доступ.

Персональные данные вне Учреждения могут представляться в государственные и негосударственные функциональные структуры:

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

5.2.1.Копировать и делать выписки персональных данных разрешается исключительно в служебных целях с письменного разрешения руководителя Учреждения.

5.2.2.Все работники Учреждения, допущенные к обработке, хранению, передаче и получению персональных данных подписывают обязательство о неразглашении информации, содержащей персональные данные (Приложение №5).

6.Права и обязанности субъектов персональных данных и Учреждения

6.1.В целях обеспечения защиты персональных данных работники и иные физические лица имеют право:

6.1.1.Получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

6.1.2.Осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законом;

6.1.3.Требовать уточнения, исключения или исправления неверных или неполных, неверных, устаревших, недостоверных, незаконно полученных персональных данных, а также данных, обработанных с нарушением законодательства;

6.1.4.При отказе должностного лица исключить или исправить персональные данные заявить в письменной форме о своем несогласии, представив соответствующее обоснование;

6.1.5.Дополнить персональные данные оценочного характера заявлением, выражающим его собственную точку зрения;

6.1.6.Требовать от руководителя Учреждения или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные

персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них;

6.1.7.Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке любые неправомерные действия или бездействие руководителя Учреждения или уполномоченного им лица при обработке и защите персональных данных.

6.2.Для защиты персональных данных Учреждение обязано:

6.2.1.За свой счет обеспечить защиту персональных данных от неправомерного их использования или утраты в порядке, установленном законодательством РФ;

6.2.2.Ознакомить работника или его представителей с настоящим Положением и его правами в области защиты персональных данных под расписку;

6.2.3.По письменному запросу ознакомить физических лиц, не являющихся работниками Учреждения, или в случае недееспособности либо несовершеннолетия физического лица, его законных представителей с настоящим Положением и его правами в области защиты персональных данных;

6.2.4.Осуществлять передачу персональных данных только в соответствии с настоящим Положением и законодательством Российской Федерации;

6.2.5.Предоставлять персональные данные только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей в соответствии с настоящим положением и законодательством Российской Федерации;

6.2.6.Обеспечить работниками и иным физическим лицам свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством;

6.2.7.По письменному требованию работника, иного физического лица или его законного представителя предоставить ему полную информацию о его персональных данных и обработке этих данных.

7.Защита персональных данных

7.1.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.

7.1.2.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.

7.1.3.Защита персональных данных представляет собой жестко регламентированный и динамически-технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и

конфиденциальности персональных данных и в конечном счете обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Учреждения.

7.1.4.Защита персональных данных работника или иного физического лица от неправомерного их использования или утраты должна быть обеспечена руководителем Учреждения за счет его средств в порядке, установленном федеральными законами.

7.2.«Внутренняя защита».

7.2.1.Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал Учреждения, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и работниками Учреждения.

7.2.2.Для обеспечения внутренней защиты персональных данных 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;

-разъяснительная работа с работниками Учреждения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

-личные дела могут выдаваться на рабочие места только руководителю Учреждения, работникам кадровой службы и в исключительных случаях, по письменному разрешению руководителя учреждения, - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

7.2.3.Защита персональных данных на электронных носителях:

-все папки, содержащие персональные данные, должны быть защищены паролем, который сообщается руководителю Учреждения.

7.3.«Внешняя защита».

7.3.1.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.

7.3.2.Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Учреждения, посетители, работники других организаций. 7.3.4.Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в Учреждении.

7.4.Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

-порядок приема, учета и контроля деятельности посетителей;

-учет и порядок выдачи удостоверений;

-технические средства охраны, сигнализации;

-порядок охраны территории, зданий, помещений, транспортных средств;

-требования к защите информации при интервьюировании и собеседованиях.

7.5.По возможности персональные данные обезличиваются.

7.6.Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители, иные физические лица могут вырабатывать совместные меры защиты персональных данных.

8.Ответственность за разглашение информации, связанной с персональными данными

8.1.Работники Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

8.2.Руководитель Учреждения за нарушение норм, регулирующих получение, обработку и защиту персональных данных, несет административную ответственность согласно Кодекса об административных правонарушениях Российской Федерации.

8.3.Неправомерный отказ руководителя Учреждения исключить или исправить персональные данные, а также любое иное нарушение прав на защиту персональных данных влечет возникновение у работника или иного физического лица права требовать устранения нарушения его прав и компенсации причиненного таким нарушением морального вреда.