

УТВЕРЖДАЮ
Директор КОГПОБУ ВПМТ



О.М. Мельников

05 сентября 2019г.

ПОЛОЖЕНИЕ
о порядке получения, обработки, защиты и хранения
персональных данных работников
Кировского областного государственного профессионального
образовательного бюджетного учреждения
«Вятско-Полянский механический техникум»
(КОГПОБУ ВПМТ)

1. Общие положения

Настоящее Положение о порядке получения, обработки, защиты и хранения персональных данных работников разработано в соответствии со следующими нормативно-правовыми актами:

- Конституцией Российской Федерации
- Трудовым кодексом РФ
- Кодексом РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»
- Указом Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»
- Уставом Кировского областного государственного профессионального образовательного бюджетного учреждения «Вятско-Полянский механический техникум» от 21.12.2015 № 5-946
- и другими действующими нормативно-правовыми актами

Настоящим Положением определяется порядок получения, обработки, защиты, хранения, передачи и любого другого использования персональных данных работников, а также ведения их личных дел в соответствии с трудовым законодательством Российской Федерации.

Цель настоящего Положения – защита персональных данных работников КОГПОБУ «Вятско-Полянский механический техникум» (далее Учреждение) от несанкционированного доступа и разглашения.

В настоящем Положении используются следующие основные понятия и термины:

- **персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации 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;

- **защита персональных данных** – комплекс мер технического, организационного и организационно-технического, правового характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных – работнику);

- **персональные данные работника** – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника;

- **общедоступные персональные данные работника** – 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;

- **работник** – физическое лицо, вступившее в трудовые отношения с работодателем (образовательным учреждением);

- **работодатель** – юридическое лицо (образовательное учреждение), вступившее в трудовые отношения с работником;

- **обработка персональных данных** – действия (операции) с персональными данными работников, обучающихся, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), уничтожение персональных данных;

- **информационная система персональных данных** – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

- **использование персональных данных** – действия (операции) с персональными данными, совершаемые работодателем (уполномоченным им лицом) в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении

работников или других лиц либо иным образом, затрагивающих права и свободы работников или других лиц;

- **конфиденциальность персональных данных** – обязательное для соблюдения работодателем или лицом, получившим доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;

- **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.

Настоящее Положение является локальным нормативным актом, который утверждается приказом руководителя Учреждения.

Настоящее Положение вступает в силу с момента его утверждения руководителем Учреждения и действует бессрочно, до замены его новым Положением. Все изменения в Положение вносятся путём издания приказа.

Все работники образовательной организации должны быть ознакомлены с настоящим Положением под роспись.

2. Сбор, обработка и защита персональных данных работника

Персональные данные работника относятся к конфиденциальной информации, то есть порядок работы с ними регламентирован действующим законодательством РФ и осуществляется с соблюдением строго определенных правил и условий.

Работники, осуществляющие обработку персональных данных, должны быть уведомлены в письменной форме о своей обязанности не разглашать персональные данные работников, к которым они получили доступ.

Общие требования обработки персональных данных работника:

Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов Российской Федерации; обучения и продвижения по службе; обеспечения личной безопасности работников; контроля количества и качества выполняемой работы и обеспечения сохранности имущества работодателя, работника и третьих лиц; заключения договоров гражданско-правового характера; обеспечения социальными льготами в соответствии с законодательством и нормативными документами техникума; осуществления материальной поддержки работников техникума; осуществления библиотечного и информационного обслуживания работников техникума; проведения предварительных и периодических медицинских осмотров работников; проведения общественно-значимых мероприятий в сфере профессионального образования (конференций, семинаров, выставок, конкурсов профессионального мастерства), культурно-массовых и физкультурно-спортивных мероприятий; ведения бухгалтерского учета; осуществления пропускного режима на территорию техникума.

При определении объема и содержания обрабатываемых персональных данных работника, Учреждение должно руководствоваться Трудовым кодексом РФ, Гражданским кодексом, Налоговым кодексом, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 06.12.2011 г. № 402-ФЗ «О бухгалтерском учете», Указом Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера», договором, заключенным между оператором и субъектом персональных данных, согласием на обработку персональных данных, а так же утвержденному Перечню персональных данных сотрудников Учреждения с местом хранения и списком допущенных лиц.

Все персональные данные работника следует получать лично у работника. 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, характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

Учреждение не имеет права получать и обрабатывать персональные данные работников о их политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых, образовательных отношений, в соответствии со статьей 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

Учреждение не имеет права получать и обрабатывать персональные данные работников о их членстве в общественных объединениях, за исключением случаев, предусмотренных действующим законодательством;

При принятии решений, затрагивающих интересы работника, Учреждение не имеет права основываться на персональных данных работника, полученных электронно или в результате их автоматизированной обработки.

Информация, содержащая персональные данные работников, используется организацией, в частности, в целях выполнения требований:

- трудового законодательства иных актов, содержащих нормы трудового права, при приеме на работу, при предоставлении гарантий и компенсаций и др.;

- налогового законодательства, в частности, в связи с исчислением и уплатой налога на доходы физических лиц;

- пенсионного законодательства при формировании и предоставлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование;

Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном действующим законодательством.

Защита персональных данных работников от неправомерного их использования или утраты должна быть обеспечена Учреждением за счет его средств в порядке, установленном действующим законодательством РФ.

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

Работники не должны отказываться от своих прав на сохранение и защиту тайны. Если в трудовом договоре будет содержаться норма об отказе работника от данного права, то в этой части трудовой договор будет считаться недействительным.

3. Состав персональных данных

2.1. Под персональными данными работников понимается информация, необходимая учреждению в связи с трудовыми отношениями и касающаяся конкретного работника, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. К персональным данным работников относятся:

- фамилия, имя, отчество
- дата, год, месяц и место рождения;
- адрес;
- семейное положение;
- образование ;
- профессия;
- доходы;
- состояние здоровья;
- идентификационный номер налогоплательщика;
- паспортные данные;
- данные трудовой книжки;
- данные страхового свидетельства обязательного пенсионного страхования;

- гражданство;
- пол;
- фотография;
- место учебы;
- данные свидетельства о рождении детей;
- сведения о социальных льготах, пенсионном обеспечении и страховании;
- имущественное положение;
- сведения о составе семьи и членах семьи;
- образование (сведения об образовательном учреждении, форма обучения, срок обучения, данные документа об образовании, специальности, квалификации);
- должность (квалификационный уровень);
- данные документов о профессиональной переподготовке, повышении квалификации, стажировке;
- данные документа о подтверждении специальных знаний;
- сведения о владении иностранными языками;
- сведения о наградах и званиях;
- данные документов об инвалидности;
- данные медицинского заключения;
- сведения о воинском учете (отношение к воинской обязанности, данные военного билета и приписного удостоверения);
- стаж работы;
- реквизиты лицевого счета в банковских учреждениях;
- номера телефонов;
- данные о наличии (отсутствии судимости).
- информация, содержащаяся в приказах по личному составу, приказах о предоставлении отпусков, приказах о взысканиях, приказах о поощрении и премировании;
- информация, содержащаяся в графике отпусков, служебных характеристиках, рекомендациях и т.п.

4. Личное дело работника

При поступлении на работу работник предоставляет персональные данные о себе в документированной форме. А именно:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство обязательного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании и (или) о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;
- справку о наличии (отсутствии) судимости и (или) факта уголовного преследования;
- идентификационный номер налогоплательщика;
- медицинскую книжку.

После того, как будет принято решение о приеме работника на работу, а также впоследствии в процессе трудовой деятельности к документам, содержащим персональные данные работника, также будут относиться:

- дополнительные соглашения к трудовому договору;
- заявления о переводе, увольнении, изменении персональных данных;
- копии приказов по личному составу, которые касаются работника;
- аттестационный лист работника, прошедшего аттестацию;
- иные документы.

После издания приказа о приеме на работу формируется личное дело работников.

Личное дело ведется на протяжении всей трудовой деятельности работников. Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

5. Хранение персональных данных работника

5.1. Сведения о работниках организации хранятся на бумажных носителях и в информационных системах.

При работе специалистов, документы на бумажных носителях, находящиеся в работе, могут находиться на рабочих столах или в специальных папках только в течение рабочего дня. По окончании рабочего дня данные документы должны убираться в закрывающиеся шкафы.

Сведения о работниках организации могут также храниться на электронных носителях, доступ к которым ограничен паролем.

Работодатель обеспечивает ограничение доступа к персональным данным работников лицам, не уполномоченным законом либо работодателем для получения соответствующих сведений.

Право внутреннего доступа к персональным данным работников образовательного учреждения имеют работники, уполномоченные в соответствии с приказом на получение и доступ к персональным данным работников;

При получении сведений, составляющих персональные данные работника, указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций, заданий.

5.2. Помещения, в которых хранятся персональные данные субъектов, оборудуются надежными замками.

Для хранения персональных данных используются специально оборудованные шкафы или сейфы, которые запираются на ключ.

Помещения, в которых хранятся персональные данные субъектов, в рабочее время при отсутствии в них работников должны быть закрыты.

Проведение уборки помещений, в которых хранятся персональные данные, должно производиться в присутствии соответствующих работников.

6. Защита информации о персональных данных

Сотрудники, ответственные за информатизацию в Учреждении (обеспечивают следующие меры по защите хранящейся на сервере информации:

- ограничение сетевого доступа на сервер для определенных пользователей;
- организацию контроля технического состояния серверов и уровней защиты и восстановления информации;
- проведение регулярного резервного копирования информации;
- ведение аудита действий пользователей и своевременное обнаружение фактов несанкционированного доступа к информации;
- сервер настроен таким образом, чтобы осуществлять возможность восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней, на любой момент времени.

Работники Учреждения, имеющие доступ к персональным данным, при пользовании доступом в сеть интернет обязаны принимать максимальные меры по обеспечению безопасности:

- использовать антивирусное программное обеспечение (с обновлением баз вирусов);
- по мере возможностей устанавливать обновление для операционной системы.

7. Политика назначения и смены паролей в Учреждении

Настоящая Политика определяет порядок обеспечения надежных средств идентификации и проверки подлинности пользователей и администраторов, хранящих и обрабатывающих

конфиденциальную информацию на автоматизированных рабочих местах (далее - АРМ) и серверах.

Ответственным за обеспечение выполнения настоящей политики является Администратор безопасности информационных систем персональных данных.

Установку первичного пароля производит Администратор безопасности информационных систем персональных данных при создании новой учётной записи. Ответственность за сохранность первичного пароля лежит на администраторе, установившем данный пароль.

При создании первичного пароля Администратор безопасности информационных систем персональных данных обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учётной записи о необходимости произвести смену пароля.

Первичный пароль не используется при сбросе забытого пароля на учётную запись, необходима установка нового пароля.

Установку основного пароля производит пользователь при первом входе в систему с новой учётной записью.

Личные пароли должны выбираться Администратором безопасности информационных систем персональных данных и пользователями с учетом следующих требований:

- длина пароля не менее шести символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ, числа, сочетания цифр и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

Пароль не должен содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков;

Содержать знаки трех из четырех перечисленных категорий: латинские заглавные буквы (от А до Z), латинские строчные буквы (от а до z), цифры (от 0 до 9), отличающиеся от букв и цифр знаки (например: !, \$, #, %);

При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях.

Пользователь несет персональную ответственность за сохранение в тайне основного пароля.

Пользователям запрещается:

- Записывать пароль и хранить его в легко доступных местах, в том числе на мониторе, рабочем столе или ящиках стола;

- сообщать пароль другим лицам;

- пересылать открытым текстом в электронных сообщениях;

- подбирать пароли других пользователей.

Пользователи обязаны сообщать Администратору безопасности информационных систем персональных данных о всех случаях попыток противоправных действий пользователей в отношении других пользователей.

Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий организации (увольнение, перевод на другую должность) должна производиться Администратором безопасности информационных систем персональных данных немедленно после окончания последнего сеанса работы данного пользователя с системой.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, перевод на другую должность) Администратора безопасности информационных систем персональных данных.

В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии условиями и требованиями настоящей Политики в зависимости от полномочий владельца скомпрометированного пароля.

Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном шкафу (ящике), сейфе с взрезным или навесным замком, либо в сейфе Администратора безопасности информационных систем персональных данных.

При возникновении нештатных ситуаций, форс-мажорных обстоятельств, которые влекут необходимость доступа к информации пользователя, отсутствующего на рабочем

месте, по решению Руководителя может быть инициирован сброс пароля данного пользователя Администратором безопасности информационных систем персональных данных и осуществлен доступ к необходимой информации. По факту такого доступа составляется акт, описывающий условия осуществления доступа, который подписывается Руководителем, Администратором безопасности информационных систем персональных данных и сотрудником, запросившим доступ.

Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администратора безопасности информационных систем персональных данных.

8. Условия использования глобальной компьютерной сети интернет и электронной почты на рабочем месте

Глобальная компьютерная сеть Интернет (далее - сеть Интернет) предоставляет доступ к ресурсам различного содержания и направленности. Системный администратор оставляет за собой право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а так же к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

Условия использования глобальной компьютерной сети интернет и электронной почты на рабочем месте предназначены для сотрудников КОГПОБУ «Вятско-Полянский механический техникум», выполнение должностных обязанностей которых связано с использованием персональных компьютеров (далее - ПК), и определяет их полномочия, обязанности и ответственность при использовании информационных ресурсов сети Интернет.

Условия использования являются обязательными для выполнения всеми сотрудниками Учреждения – пользователями сети Интернет в части, касающейся их.

Руководители структурных подразделений, пользователи и администраторы обязаны знать и выполнять нормативные правовые акты, затрагивающие вопросы информатизации, защиты информации и информационной безопасности в части соблюдения требований и ограничений по использованию информационных ресурсов.

Доступ к сети Интернет осуществляется с рабочего ПК пользователя. Ответственность за действия на компьютере другого сотрудника несёт пользователь ПК, с которого совершено это действие.

Порядок работы в сети Интернет:

Для работы в сети интернет рекомендуется использовать Браузер «Yandex», допустимо использование браузеров Mozilla Firefox, Opera и Internet Explorer.

При работе с ресурсами сети Интернет недопустимо:

-Разглашение служебной информации Учреждения, ставшей известной сотруднику по служебной необходимости либо иным путем;

-Публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, а также размещения ссылок на вышеуказанную информацию,

При работе с ресурсами сети Интернет запрещается:

-Загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

-Допускать к работе посторонних лиц;

-Использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой Учреждения;

-Передавать служебные данные через интернет-пейджеры, социальные сети и т.д.;

-Использовать для рабочих целей облачные хранилища: Яндекс.Диск, Dgorbox и т.д.;

Пользователь обязан знать и уметь пользоваться антивирусным программным обеспечением. При обнаружении вируса он должен сообщить об этом системному администратору. Пользователю запрещается производить какие-либо действия с информацией, зараженной вирусом.

Пользователь обязан информировать системного администратора о любых нарушениях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети.

Порядок работы с электронной почтой:

Для исполнения задач, связанных с производственной деятельностью сотрудникам Учреждения предоставляется доступ к системе электронной почты Учреждения. Использование системы электронной почты Учреждения в других целях – запрещено.

Электронная почта является собственностью Учреждения и может быть использована только в служебных целях.

Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

Доступ к серверу электронной почты может быть заблокирован системным администратором без предварительного уведомления, при возникновении нештатной ситуации, либо в иных случаях предусмотренных организационными документами.

Ограничения доступа.

Возможны следующие ограничения доступа к сети Интернет для пользователей:

-Ограничение доступа к сети Интернет с рабочего места;

-Ограничение доступа к внешней электронной почте: mail.ru, yandex.ru и др.;

-Ограничение к развлекательным сайтам;

-Ограничение доступа к социальным сетям: одноклассники.ru, vk.com и т.д.

9. Передача персональных данных работника

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

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 (например, несчастный случай на производстве обязывает работодателя при необходимости доставить пострадавшего в учреждение здравоохранения, немедленно проинформировать родственников пострадавшего, а также направить сообщение в органы и организации, определенные Трудовым кодексом РФ (ст. 228 ТК РФ), иными федеральными законами; о случаях острого отравления работодатель сообщает в соответствующий орган санитарно-эпидемиологического надзора).

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 подтверждения того, что это правило соблюдено;

Осуществлять передачу персональных данных работника в пределах одного работодателя в соответствии с настоящим Положением;

Разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

Потребителями персональных данных работников вне организации могут быть следующие государственные и негосударственные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- муниципальные органы власти и управления;
- страховые организации;
- другие.

Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом и настоящим Положением, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

10. Обязанности работника и работодателя в области персональных данных

В целях обеспечения достоверности персональных данных работник обязан:

- При приеме на работу предоставить полные и достоверные данные о себе;
- В случае изменения сведений, составляющих персональные данные, незамедлительно предоставить данную информацию в Учреждение.

Учреждение обязано:

- Осуществлять защиту персональных данных работников;
- Обеспечить хранение первичной учетной документации по учету труда и его оплаты, к которой, в частности, относятся документы по учету кадров, документы по учету использования рабочего времени и расчетов с работниками по оплате труда и др. При этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные;

-Заполнение документации, содержащей персональные данные работника осуществлять в соответствии с унифицированными формами первичной учетной документации по учету труда и его оплаты, утвержденными действующим законодательством РФ;

-По письменному заявлению работника не позднее трех дней со дня подачи этого заявления выдавать последнему копии документов, связанных с работой (копии приказа о приеме на работу, приказов о переводах на другую работу, приказа об увольнении с работы; выписки из трудовой книжки; справки о заработной плате, периоде работы у данного работодателя и другое). Копии документов, связанных с работой, должны быть заверены надлежащим образом и предоставляться работнику безвозмездно;

-Вести учет передачи персональных данных работника третьим лицам путем ведения соответствующего журнала, отражающего сведения о поступившем запросе (кто является отправителем запроса, дата его поступления работодателю), дату ответа на запрос, какая именно информация была передана либо отметку об отказе в ее предоставлении, либо ограничиваться помещением в личное дело работника выписок, копий документов и т.п., отражающих сведения о поступившем запросе и результатах его рассмотрения;

-В целях обеспечения сохранности документов по личному составу увольняемых работников в случае реорганизации и ликвидации организации, а также социальной защищенности граждан, выполняющих работу по трудовому договору, включать в свои учредительные документы правила учета и сохранности документов по личному составу, а также своевременной передачи их на государственное хранение при реорганизации или ликвидации юридического лица.

В случае реорганизации или ликвидации организации учет и сохранность документов по личному составу, порядок передачи их на государственное хранение осуществлять в соответствии с Законодательством и правилами, предусмотренными Учредительными документами.

11. Права работников Учреждения в области защиты персональных данных

В целях обеспечения защиты персональных данных, хранящихся в Учреждении, работники имеют право на:

- Полную информацию об их персональных данных и обработке этих данных, в частности имеют право знать, кто и в каких целях использует или использовал его персональные данные;

- Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника за исключением случаев, предусмотренных федеральным законом;

- Определение представителей для защиты своих персональных данных; Доступ к относящимся к ним медицинским данным;

- Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований настоящего Положения. При отказе Учреждения исключить или исправить персональные данные работник имеет право заявить в письменной форме о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

- Требование об извещении Учреждением всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника обо всех произведенных в них исключениях, исправлениях или дополнениях;

- Обжалование в суд любых неправомерных действий или бездействия Учреждения при обработке и защите персональных данных.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

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

Если права и законные интересы работника были нарушены в связи с разглашением информации, содержащей его персональные данные, или иным неправомерным использованием такой информации, он вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с иском о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации.

12. Способы защиты персональных данных. Уничтожение персональных данных

Защита персональных данных работников представляет собой регламентированный технологический, организационный и иной процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных работников образовательного учреждения и обеспечивающий надежную безопасность информации.

Защита персональных данных работников от неправомерного их использования или утраты обеспечивается Учреждением за счет его средств в порядке, установленном федеральным законом.

Для обеспечения внутренней защиты персональных данных работников руководитель Учреждения предпринимает следующие меры:

- регламентирует состав работников, функциональные обязанности которых требуют соблюдения режима конфиденциальности;
- избирательно и обоснованно распределяет документы и информацию между работниками, имеющими доступ к персональным данным;
- своевременно обеспечивает работников информацией о требованиях законодательства по защите персональных данных;
- обеспечивает организацию порядка уничтожения информации;
- проводит разъяснительную работу с работниками, имеющими доступ к персональным данным, по предупреждению утраты сведений при работе с персональными данными.

Защита сведений, хранящихся в электронных базах данных, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается разграничением прав доступа с использованием учетной записи и системой паролей.

Для обеспечения внешней защиты персональных данных работников образовательное учреждение:

- обеспечивает порядок приема, учета и контроля деятельности посетителей;
- обеспечивает охрану территории, зданий, помещений.

Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников. (Приложение 3).

В случае выявления недостоверных персональных данных работника или неправомерных действий с ними на период проверки Учреждение, в лице ответственных лиц обязано осуществить блокирование персональных данных работника с момента обращения его самого либо получения запроса уполномоченного органа по защите прав субъектов.

При выявлении неправомерных действий с персональными данными работника Учреждение, в лице ответственных лиц обязано устранить допущенные нарушения не более трех рабочих дней с даты такого выявления.

В случае отзыва работником согласия на обработку своих персональных данных Учреждение обязано прекратить обработку персональных данных работника и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между работником и работодателем. (Приложение 4).

Уничтожение персональных данных

Уничтожение персональных данных может быть произведено без уничтожения носителя персональных данных.

Необходимость уничтожения носителя персональных данных появляется в случае:

- физической неисправности носителя;
- списания носителя с бухгалтерского учета Учреждения.

Уничтожение персональных данных без уничтожения носителя производится в случае:

- необходимости уничтожить персональные данные по требованию субъекта;
- очистке файлов носителя типа ППЗУ после предоставления персональных данных;
- иной необходимости уничтожения персональных данных.

В случае отсутствия необходимости в уничтожении носителя уничтожение персональных данных производится незамедлительно.

Уничтожение носителей информации проводится в присутствии комиссии, назначенной приказом руководителя Учреждения (по форме, прилагаемой к Положению «Об уничтожении персональных данных» КОГПОБУ «Вятско-Полянский механический техникум», и сопровождается составлением Акта об уничтожении носителя информации.

Ответственность за уничтожение носителей возлагается на ответственного за организацию обработки персональных данных.

Уничтожение персональных данных на бумажных носителях:

Уничтожение персональных данных с бумажного носителя без уничтожения самого носителя производится любым подходящим способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки остальных данных бумажного носителя (удаление, вымарывание). В случае согласия субъекта персональных данных допускается уничтожение его персональных данных путем закрашивания.

Уничтожение персональных данных на бумажных и машинных носителях производится в соответствии с порядком, установленным Положением «Об уничтожении персональных данных» КОГПОБУ «Вятско-Полянский механический техникум».

13. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работников

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника привлекаются к дисциплинарной и материальной ответственности в порядке, установленном ТК РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», кодексом РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Лица, в обязанность которых входит ведение персональных данных работников, подписывают Обязательство «О неразглашении персональных данных» (Приложение 3).

За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера несут дисциплинарную и материальную ответственность в порядке, установленном действующим законодательством РФ.

Лица, в обязанность которых входит ведение персональных данных работников, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

14. Заключительные положения

Учреждение обязано ознакомить сотрудников, в обязанности которых входит получение, обработка, защита и хранение персональных данных работников и обучающихся КОГПОБУ ВПМТ, с настоящим Положением, а также с внесенными в него изменениями и дополнениями под роспись (Приложение 1).

Изменения и дополнения в настоящее Положение вносятся в порядке, установленном действующим законодательством РФ для принятия локальных нормативных актов.

Положение вступает в силу с момента утверждения и действует до принятия нового.

**Перечень лиц, в обязанности которых входит получение, обработка, защита
и хранение персональных данных работников и обучающихся КОГПОБУ
ВПМТ**

1. Директор;
2. Зам. директора по УР;
3. Зам. директора по ВР;
4. Зам. директора по УПР;
5. Главный бухгалтер;
6. Бухгалтер;
7. Начальник центра информационных технологий;
8. Начальник административно-хозяйственного отдела;
9. Начальник отдела кадров;
10. Инспектор отдела кадров;
11. Инженер по охране труда;
12. Инженер-электроник;
13. Методист;
14. Секретарь руководителя;
15. Секретарь учебной части;
16. Диспетчер;
17. Лаборант;
18. Архивариус;
19. Преподаватель-организатор ОБЖ;
20. Руководитель физического воспитания;
21. Преподаватель;
22. Мастер производственного обучения;
23. Педагог-психолог;
24. Социальный педагог;
25. Заведующий МУАП сварки;
26. Библиотекарь;
27. Заведующий отделением подготовки водителей ТС;
28. Ответственный за обеспечение БДД, контролер (к персональным данным, касающимся состояния здоровья водителей);
29. Контролер технического состояния ТС (к персональным данным, касающимся состояния здоровья водителей);
30. Сторож (вахтер);
31. Охранник ЧОП.

Приложение 2
Согласие работника на обработку
персональных данных

**СОГЛАСИЕ
на обработку персональных данных**

Во исполнение требований Федерального закона «О персональных данных» № 152-ФЗ от 27.07.2006 г., работник

(Ф.И.О.)

именуемый (ая) в дальнейшем Субъект, разрешает Кировскому областному государственному профессиональному образовательному бюджетному учреждению «Вятско-Полянский механический техникум», именуемый в дальнейшем Оператор, обработку персональных данных (список приведен в пункте 3 настоящего Согласия) на следующих условиях:

1. Субъект дает согласие на обработку Оператором своих персональных данных, то есть совершение, следующих действий: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, а также право на передачу такой информации третьим лицам, если это необходимо для организационной и финансово-экономической деятельности Оператора.

2. Целью обработки персональных данных является получение информации, необходимой работодателю в связи осуществлением трудовых отношений. Оператор обязуется использовать данные Субъекта в соответствии с действующим законодательством Российской Федерации.

3. Перечень персональных данных передаваемых Оператору на обработку: фамилия, имя и отчество; дата рождения; место рождения; биографические сведения; сведения о местах обучения (город, образовательное учреждение, сроки обучения); сведения о местах работы (город, название организации, должность, сроки работы); сведения о месте регистрации, проживания; сведения о документах об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки; сведения, необходимые для ведения воинского учета; семейное, социальное, имущественное положение; паспортные данные; данные о трудовом стаже; о состоянии здоровья; идентификационный номер налогоплательщика; номер страхового свидетельства государственного пенсионного страхования; контактная информация; доходы; другая информация (согласно статье 3 ФЗ РФ от 27.07.2006 г. «О персональных данных» № 152-ФЗ).

4. Субъект персональных данных, по письменному запросу, имеет право на получение информации, касающейся обработки его персональных данных (в соответствии с п.4 ст. 14 ФЗ №152 от 27.07.2006 г.).

5. В случае выявления неправомерных действий с персональными данными Оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязуется устранить допущенные нарушения.

В случае отзыва Субъектом персональных данных согласия на обработку своих персональных данных Оператор обязуется 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.

6. Настоящее согласие действует в течение сроков хранения личной карточки Ф - Т2 и (или) личного дела Субъекта.

7. Подписи сторон.

Субъект		Оператор	
паспорт		Кировское областное государственное профессиональное образовательное бюджетное учреждение «Вятско-Полянский механический техникум»	
выдан			
дата выдачи		Директор	О.М. Мельников
адрес			

С положением о работе с персональными данными работников и обучающихся ознакомлен, с порядком обработки моих персональных данных согласен _____ (подпись).

Приложение 3

Обязательство о неразглашении персональных данных

ОБЯЗАТЕЛЬСТВО о неразглашении персональных данных

Я, _____,
(ФИО)

_____,
(паспортные данные)

работающий в « _____ »
(наименование организации)

на должности _____

понимаю, что в соответствии с трудовым договором, должностной инструкцией получаю доступ к персональным данным физических лиц, а именно:

- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- 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 и трудовые книжки сотрудников;
- личные дела учащихся;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке, их аттестации;
- копии отчетов, направляемые в органы статистики.

Я также понимаю, что во время исполнения своих обязанностей мне предстоит заниматься сбором, обработкой, накоплением, хранением и обновлением персональных данных физических лиц.

Я обязуюсь хранить в тайне известные мне конфиденциальные сведения, информировать руководителя организации о фактах нарушения порядка обращения с персональными данными, о ставших мне известными попытках несанкционированного доступа к информации.

Я обязуюсь соблюдать правила пользования документами, порядок их учета и хранения, обеспечивать в процессе работы сохранность информации, содержащейся в них, от посторонних лиц, знакомиться только с теми служебными документами, к которым получаю доступ в силу исполнения своих служебных обязанностей.

Я понимаю, что разглашение такого рода информации может нанести прямой или косвенный ущерб физическим лицам. В связи с этим даю обязательство при обработке персональных данных соблюдать все описанные в Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлении Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и других нормативных актах, требования.

Я предупрежден(а) о том, что в случае разглашения мной персональных данных или их утраты я несу ответственность в соответствии с действующим законодательством РФ.

« ____ » _____ 20__ г.

подпись

расшифровка подписи

Приложение 4

Отзыв согласия на обработку персональных данных

Директору КОГПОБУ «Вятско-Полянский механический техникум»

От: _____

Зарегистрированного по адресу:

Паспорт: серия _____ № _____

Выдан:

Отзыв согласия на обработку персональных данных

Я, _____, в соответствии с п.2. ст.9. Федерального закона «О персональных данных» № 152-ФЗ от 27.07.2006 года отзываю у КОГПОБУ «Вятско-Полянский механический техникум» согласие на обработку моих персональных данных.

Прошу прекратить обработку моих персональных данных в течение тридцати дней с момента поступления настоящего отзыва.

Дата

подпись

расшифровка

Приложение 5
Согласие на использование изображения
работника

СОГЛАСИЕ
на использование изображения работника

г. Вятские Поляны

«___» _____ 20__

Я, _____

(Ф.И.О., паспортные данные, адрес регистрации)

_____ года рождения, в соответствии со статьей 152.1 Гражданского Кодекса РФ, являясь: совершеннолетним (ей), в соответствии с действующим законодательством РФ, настоящим документом даю согласие на использование без выплаты вознаграждения моих изображений _____

(Ф.И.О. автора изображений)

КОГПОБУ «Вятско-Полянский механический техникум» (ОГРН 1024300609266)

(полное наименование правообладателя, с указанием ОГРН)

именуемому далее «Правообладатель».

Настоящее Согласие предоставляется на все мои изображения, полученные в процессе съемки

_____ *(объект съемки)*

в период с _____ по _____.

Даю согласие на использование моих изображений в рекламных, информационных и иных материалах, размещаемых на наружных и внутренних стендах, в печатных изданиях, в сети интернет на территории Российской Федерации.

Настоящее согласие дает Правообладателю право обнародовать и в дальнейшем использовать мои изображения полностью или фрагментарно: воспроизводить, осуществлять публичный показ, импортировать оригиналы или экземпляры изображений в целях распространения, предоставлять оригиналы или экземпляры изображений, сообщать в эфир и по кабелю, перерабатывать, доводить до всеобщего сведения.

Изображения не могут быть использованы Правообладателем способами, порочащими честь, достоинство и деловую репутацию.

Изображения могут быть использованы до дня отзыва настоящего согласия в письменной форме.

Ф.И.О.

Подпись