

УТВЕРЖДАЮ

директор ГБУ «ПШЦ»
Горбанёва Л.А.

« 01» сентября 2022 г

**ПОЛИТИКА
ГБУ «ПШЦ» г.о. Тольятти
в отношении обработки персональных данных
сотрудников
обучающихся, воспитанников и их родителей (законных
представителей)**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение в отношении обработки персональных данных разработано на основании ст. 24 Конституции РФ, гл. 14 Трудового кодекса РФ, Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информатизации и защите информации» и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Целью Положения является защита персональных данных работников, обучающихся, воспитанников, их родителей (законных представителей) от несанкционированного доступа, неправомерного их использования или утраты.

1.3. Положение определяет порядок работы (получение, обработка, использование, хранение и т.д.) с персональными данными работников, обучающихся, воспитанников, их родителей (законных представителей) и гарантии конфиденциальности предоставленных сведений.

1.4. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.5. Политика определяется и вводится в действие приказом директора ГБУ «ППЦ» и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников, обучающихся, воспитанников, их родителей (законных представителей).

1.6. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.2. В состав персональных данных работника входят:

- паспортные данные;
- анкетные и биографические данные;
- сведения об образовании и специальности;

- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- сведения о воинском учете;
- сведения о социальных льготах;
- наличие судимостей;
- адрес места жительства;
- номер телефона;
- адрес личной электронной почты;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- результаты медицинских обследований работников на предмет годности к осуществлению трудовых обязанностей.

2.3. В состав персональных данных обучающихся, воспитанников, их родителей (законных представителей) входят:

- паспортные данные и/или данные свидетельства о рождении;
- сведения об образовании и специальности;
- социальный статус семьи;
- адрес прописки (проживания), номер телефона;
- место учебы, работы членов семьи;
- заключение ПМПК;
- иные документы, предусмотренные законодательством РФ.

3. ПОЛУЧЕНИЕ, ОБРАБОТКА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Получение, обработка, хранение и любое другое использование персональных данных работников, обучающихся, воспитанников, их родителей (законных представителей) может осуществляться исключительно в целях соблюдения законодательства Российской Федерации

3.2. Персональные данные работника, обучающихся, воспитанников, их родителей (законных представителей) следует получать непосредственно у субъекта персональных данных.

3.3. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.4. Хранение персональных данных должно происходить в порядке, исключающем их утрату или неправомерное использование.

4. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

4.1. Внутренний доступ.

4.1.1. Право доступа к персональным данным имеют:

- директор;
- заместители директора (в соответствии с функционалом);
- субъект персональных данных;
- социальный педагог (с функционалом специалиста по кадрам);
- работники бухгалтерии (к данным, которые необходимы для выполнения конкретных функций);
- ответственные за обработку персональных данных.

Право получения документов, содержащих персональные данные непосредственно на рабочее место имеет директор ГБУ «ППЦ». По письменному распоряжению директора работник, ответственный за работу с соответствующими документами, обязан лично передать требуемые документы непосредственно директору.

4.1.2. Заместители директора имеют право ознакомиться с документами, содержащими персональные данные, в кабинете и в присутствии сотрудника, ответственного за работу с соответствующими документами.

4.1.3. Субъект персональных данных имеет право ознакомиться с документами, содержащими его персональные данные, в кабинете и в присутствии сотрудника, ответственного за работу с соответствующими документами.

4.2. Внешний доступ.

4.2.1. К лицам, которым могут быть переданы персональные данные вне организации, при условии соблюдения требований законодательства, относятся:

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

4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

5. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. При передаче персональных данных работников, обучающихся, воспитанников, их родителей (законных представителей) оператор обязан:

- не сообщать персональные данные третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные в коммерческих целях;
- предупредить лиц, получающих персональные данные работников, обучающихся, воспитанников, их родителей (законных представителей), 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, получающие персональные данные, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

- 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 конкретных функций.

5.2. Копирование и выписка персональных данных работников, обучающихся, воспитанников, их родителей (законных представителей) разрешаются исключительно в служебных целях по письменному запросу и с разрешения директора.

5.3. Сотрудникам, имеющим доступ к персональным данным работника, запрещается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу.

6. ПОРЯДОК ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. 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.

6.2. 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.

6.3. 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 организации.

6.4. Защита персональных данных работников, обучающихся, воспитанников, их родителей (законных представителей) от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств и в порядке, установленном федеральным законом.

6.5. Внутренняя защита.

6.5.1. Для обеспечения внутренней защиты персональных данных необходимо соблюдать следующие меры:

- 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 сохранению 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 с доступом к базам данных;
- организация процесса уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения, цель которой - предупредить утрату ценных сведений при работе с конфиденциальными документами.

6.5.2. Все файлы, содержащие персональные данные работников, обучающихся, воспитанников, их родителей (законных представителей) в электронном виде, должны быть защищены паролем.

6.6. Внешняя защита.

6.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладеть персональными данными. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания документа и др.

6.6.2. Под посторонним лицом понимается любое лицо, не являющееся работником ГБУ «ППЦ».

6.6.3. Для обеспечения внешней защиты персональных данных работника в ГБУ «ППЦ» введен пропускной режим, ведется учет посетителей с применением системы видеонаблюдения на входе.

6.7. Все лица, в должностные обязанности которых входит получение, обработка и защита персональных данных работника, при приеме на работу обязаны подписать обязательство о неразглашении персональных данных работника.

6.8. По возможности персональные данные обезличиваются.

6.9. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут выработать совместные меры защиты персональных данных работников.

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

7.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.3. Директор, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.4. Каждый сотрудник, получающий для работы конфиденциальный документ, несет личную ответственность за сохранность носителя и конфиденциальность информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом РФ дисциплинарные взыскания.

7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях РФ.

7.5.3. Нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения, влечет привлечение виновного к ответственности в соответствии с Уголовным кодексом РФ.

7.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

7.7. Защита прав работника, установленных настоящим Положением и законодательством Российской Федерации, осуществляется судом в целях пресечения неправомерного использования персональных данных работника, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.