

ПРИНЯТО:

на Общем собрании работников
ГБПОУ РО «ДонТКИиБ»
(наименование общеобразовательной организации)

Протокол № 8 от 30.08. 2025г.

Председатель  / Т.Ю.Пойманова /
подпись расшифровка подписи

УТВЕРЖДЕНО:

Директор ГБПОУ РО «ДонТКИиБ»

 / А.А.Санжаров /
подпись расшифровка подписи

03.09.2025 год

Положение о защите персональных данных работников ГБПОУ РО «ДонТКИиБ»

1. Общие положения

1.1 Настоящее Положение разработано в соответствии со статьей 24 Конституции Российской Федерации, Трудовым кодексом Российской Федерации, Федеральными законами от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» с изменениями от 23 ноября 2024 года, от 27 июля 2006 года № 152-ФЗ «О персональных данных» с изменениями от 8 августа 2024 года, Приказом Министерства цифрового развития, связи и массовых коммуникаций РФ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 года № 179 «Об утверждении требований к подтверждению уничтожения персональных данных», Федеральным законом № 273-ФЗ от 29.12.2012 «Об образовании в Российской Федерации» с изменениями от 31 июля 2025 года, а также Уставом техникуме и другими нормативными правовыми актами Российской Федерации, регламентирующими деятельность организаций, осуществляющих образовательную деятельность.

1.2. Данное Положение разработано с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну работников техникуме от несанкционированного доступа, неправомерного их использования или утраты.

1.3. Настоящее Положение регулирует отношения, связанные с обработкой персональных данных работников и гарантии конфиденциальности сведений о работнике, предоставленных работником работодателю, а также устанавливает ответственности должностных лиц, имеющих доступ к персональным данным работников техникума.

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

1.5. **Оператор** — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.6. **Обработка персональных данных** — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.7. **Автоматизированная обработка персональных данных** — обработка персональных данных с помощью средств вычислительной техники.

1.8. **Распространение персональных данных** — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.9. **Предоставление персональных данных** — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.10. **Блокирование персональных данных** — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.11. **Уничтожение персональных данных** — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

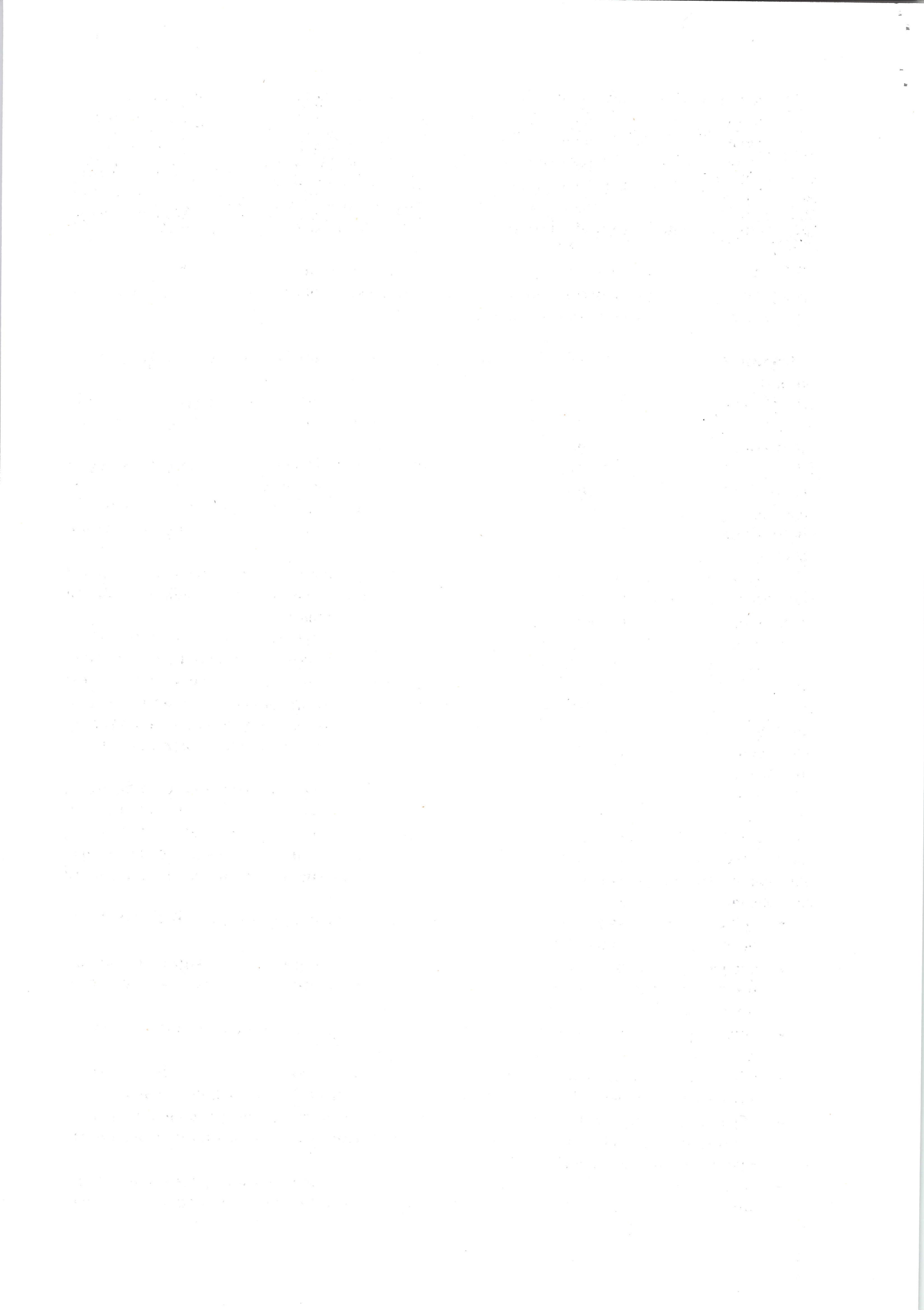
1.12. **Обезличивание персональных данных** — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

1.13. **Информационная система персональных данных** — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.14. **Общедоступные данные** — сведения общего характера и иная информация, доступ к которой не ограничен.

1.15. К персональным данным работника, получаемым и подлежащим хранению у работодателя в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения, содержащиеся в личных делах работников:

- паспортные данные работника;
- ИНН;
- копия страхового свидетельства государственного пенсионного страхования;
- документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа;
- копия документа воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);
- копия документа об образовании, квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);
- анкетные данные, заполненные работником при поступлении на работу или в процессе работы (в том числе — автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);
- документы о возрасте малолетних детей и месте их обучения;
- документы о состоянии здоровья детей и других родственников (включая справки об инвалидности, о наличии хронических заболеваний);
- документы о состоянии здоровья (сведения об инвалидности, о беременности и т.п.);
- иные документы, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены работником при заключении трудового договора или в период его действия (включая медицинские заключения, предъявляемые работником при прохождении обязательных предварительных и периодических медицинских осмотров);
- трудовой договор;
- заключение по данным психологического исследования (если такое имеется);
- копии приказов о приеме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;
- личная карточка по форме Т-2;
- заявления, объяснительные и служебные записки работника;



- документы о прохождении работником аттестации, повышения квалификации;
- иные документы, содержащие сведения о работнике, нахождение которых в личном деле работника необходимо для документального оформления трудовых правоотношений с работником (включая приговоры суда о запрете заниматься педагогической деятельностью или занимать руководящие должности).

1.16. Размещение на официальном сайте фотографий работников, видео с работниками сотрудники разрешают путем предоставления согласия на обработку персональных данных в техникуме.

1.17. Персональные данные работников техникума являются конфиденциальной информацией и не могут быть использованы сотрудниками организации, осуществляющей образовательную деятельность в личных целях.

2. Общие требования при обработке персональных данных работника и гарантии их защиты

2.1. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

2.1.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.1.2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться 24 статьей Конституцией Российской Федерации, 65 статьей Трудового Кодекса и иными федеральными законами.

2.1.3. Все персональные данные работника следует получать у него самого. 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, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

2.1.4. Работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся (в соответствии со статьей 10 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных») к специальным категориям персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, если:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных в п.2.2 данного Положения;
- обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;
- обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года N 8-ФЗ "О Всероссийской переписи населения";
- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья

или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;
- обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;
- обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;
- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;
- обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

2.1.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым Кодексом или иными федеральными законами.

2.1.6. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

2.1.7. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном Трудовым Кодексом и иными федеральными законами.

2.1.8. Работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

2.1.9. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

2.1.10. Работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

1. The first part of the document discusses the importance of maintaining accurate records of all transactions and activities. It emphasizes that proper record-keeping is essential for transparency and accountability, particularly in financial matters. The text suggests that organizations should implement robust systems to track income, expenses, and assets, ensuring that all data is up-to-date and easily accessible.

2. The second section focuses on the role of internal controls in preventing fraud and mismanagement. It highlights that strong internal controls are not only a defense against external threats but also a means to ensure the integrity of internal operations. The document recommends that organizations should regularly review and update their internal control systems to adapt to changing risks and regulatory requirements.

3. The third part of the document addresses the importance of communication and collaboration within an organization. It states that effective communication is key to ensuring that all team members are aligned with the organization's goals and objectives. The text encourages the use of various communication channels, including meetings, reports, and digital tools, to facilitate the flow of information and foster a collaborative work environment.

4. The fourth section discusses the need for continuous improvement and innovation. It argues that organizations should not be satisfied with the status quo but should actively seek ways to enhance their processes, products, and services. The document suggests that organizations should encourage a culture of innovation where employees are empowered to提出新想法 and implement improvements that drive the organization forward.

5. The fifth part of the document touches upon the importance of ethical considerations in business operations. It stresses that organizations have a responsibility to act ethically and transparently, not only to their stakeholders but also to the wider community. The text recommends that organizations should establish clear ethical guidelines and ensure that all employees are trained to understand and adhere to these principles.

6. The final section of the document provides a summary of the key points discussed and offers some concluding thoughts. It reiterates that success in business is not solely determined by financial performance but also by the organization's ability to maintain high standards of integrity, transparency, and ethical conduct. The document concludes by encouraging organizations to embrace these principles as a foundation for long-term success and sustainable growth.

2.2. Согласно ст.10.1 Федерального закона «О персональных данных», особенностями обработки персональных данных, разрешенных субъектом персональных данных для распространения являются:

2.2.1. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Работник образовательной организации (оператор) обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

2.2.2. В случае раскрытия персональных данных неопределенному кругу лиц самим субъектом персональных данных без предоставления оператору согласия, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.

2.2.3. В случае, если персональные данные оказались раскрытыми неопределенному кругу лиц вследствие правонарушения, преступления или обстоятельств непреодолимой силы, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.

2.2.4. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных согласился с распространением персональных данных, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без права распространения.

2.2.5. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных не установил запреты и условия на обработку персональных данных, предусмотренные п.2.2.9 настоящего Положения, или если в предоставленном субъектом персональных данных таком согласии не указаны категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты в соответствии с п.2.2.9 настоящего Положения, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с персональными данными неограниченному кругу лиц.

2.2.6. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору:

- непосредственно;
- с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

2.2.7. Правила использования информационной системы уполномоченного органа по защите прав субъектов персональных данных, в том числе порядок взаимодействия субъекта персональных данных с оператором, определяются уполномоченным органом по защите прав субъектов персональных данных.

2.2.8. Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

2.2.9. В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных

The first part of the document discusses the importance of maintaining accurate records of all transactions and activities. It emphasizes the need for transparency and accountability in financial reporting. The second part outlines the various methods used to collect and analyze data, including surveys, interviews, and focus groups. The third part presents the results of the study, showing a clear trend towards increased participation in community programs. The final part concludes with recommendations for future research and implementation strategies.

The data collected from the surveys and interviews indicates a significant increase in the number of participants in the community programs over the past year. This suggests that the programs are effective in attracting and retaining members. The focus group discussions provided valuable insights into the challenges faced by participants and the factors that influence their decision to join and stay in the programs. These findings are crucial for developing targeted interventions to address the identified issues.

Based on the results, it is recommended that the community programs be expanded to reach a larger audience. This can be achieved through various strategies, such as increasing the frequency of meetings, providing more resources, and offering incentives for participation. Additionally, it is important to continue monitoring the progress of the programs and conducting regular evaluations to ensure their effectiveness and sustainability.

In conclusion, the study highlights the importance of community programs in promoting social cohesion and improving the quality of life for residents. The findings provide a solid foundation for developing and implementing effective strategies to enhance the impact of these programs. Further research is needed to explore the long-term effects of the programs and to identify best practices for their implementation.

оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ оператора в установлении субъектом персональных данных запретов и условий не допускается.

2.2.10. Оператор обязан в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения.

2.2.11. Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

2.2.12. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.

2.2.13. Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления оператору требования, указанного в п.2.2.12 настоящего Положения.

2.2.14. Субъект персональных данных вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения п.2.2 данного Положения или обратиться с таким требованием в суд. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования субъекта персональных данных или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

2.2.15. Требования п.2.2 настоящего Положения не применяются в случае обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на государственные органы, муниципальные органы, а также на подведомственные таким органам организации функций, полномочий и обязанностей.

2.3. Общеобразовательная организация определяет объем, содержание обрабатываемых персональных данных работников, руководствуясь Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

2.4. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

2.5. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.6. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения,

the first of these is the fact that the
the second is the fact that the
the third is the fact that the
the fourth is the fact that the
the fifth is the fact that the
the sixth is the fact that the
the seventh is the fact that the
the eighth is the fact that the
the ninth is the fact that the
the tenth is the fact that the
the eleventh is the fact that the
the twelfth is the fact that the
the thirteenth is the fact that the
the fourteenth is the fact that the
the fifteenth is the fact that the
the sixteenth is the fact that the
the seventeenth is the fact that the
the eighteenth is the fact that the
the nineteenth is the fact that the
the twentieth is the fact that the
the twenty-first is the fact that the
the twenty-second is the fact that the
the twenty-third is the fact that the
the twenty-fourth is the fact that the
the twenty-fifth is the fact that the
the twenty-sixth is the fact that the
the twenty-seventh is the fact that the
the twenty-eighth is the fact that the
the twenty-ninth is the fact that the
the thirtieth is the fact that the
the thirty-first is the fact that the
the thirty-second is the fact that the
the thirty-third is the fact that the
the thirty-fourth is the fact that the
the thirty-fifth is the fact that the
the thirty-sixth is the fact that the
the thirty-seventh is the fact that the
the thirty-eighth is the fact that the
the thirty-ninth is the fact that the
the fortieth is the fact that the
the forty-first is the fact that the
the forty-second is the fact that the
the forty-third is the fact that the
the forty-fourth is the fact that the
the forty-fifth is the fact that the
the forty-sixth is the fact that the
the forty-seventh is the fact that the
the forty-eighth is the fact that the
the forty-ninth is the fact that the
the fiftieth is the fact that the
the fifty-first is the fact that the
the fifty-second is the fact that the
the fifty-third is the fact that the
the fifty-fourth is the fact that the
the fifty-fifth is the fact that the
the fifty-sixth is the fact that the
the fifty-seventh is the fact that the
the fifty-eighth is the fact that the
the fifty-ninth is the fact that the
the sixtieth is the fact that the
the sixty-first is the fact that the
the sixty-second is the fact that the
the sixty-third is the fact that the
the sixty-fourth is the fact that the
the sixty-fifth is the fact that the
the sixty-sixth is the fact that the
the sixty-seventh is the fact that the
the sixty-eighth is the fact that the
the sixty-ninth is the fact that the
the seventieth is the fact that the
the seventy-first is the fact that the
the seventy-second is the fact that the
the seventy-third is the fact that the
the seventy-fourth is the fact that the
the seventy-fifth is the fact that the
the seventy-sixth is the fact that the
the seventy-seventh is the fact that the
the seventy-eighth is the fact that the
the seventy-ninth is the fact that the
the eightieth is the fact that the
the eighty-first is the fact that the
the eighty-second is the fact that the
the eighty-third is the fact that the
the eighty-fourth is the fact that the
the eighty-fifth is the fact that the
the eighty-sixth is the fact that the
the eighty-seventh is the fact that the
the eighty-eighth is the fact that the
the eighty-ninth is the fact that the
the ninetieth is the fact that the
the ninety-first is the fact that the
the ninety-second is the fact that the
the ninety-third is the fact that the
the ninety-fourth is the fact that the
the ninety-fifth is the fact that the
the ninety-sixth is the fact that the
the ninety-seventh is the fact that the
the ninety-eighth is the fact that the
the ninety-ninth is the fact that the
the hundredth is the fact that the

изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3. Хранение и использование персональных данных

3.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обработываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Персональные данные работников организации хранятся на бумажных и электронных носителях (к доступу имеется определенный код), в специально предназначенных для этого помещениях.

3.3. В процессе хранения персональных данных работников должны обеспечиваться:

- требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;
- сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящим Положением;
- контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

3.4. Доступ к персональным данным работников имеют:

- директор;
- заместители директора;
- руководители структурного подразделения;
- секретарь учебной части;
- специалист по кадрам;
- иные работники, определяемые приказом директора техникума в пределах своей компетенции.

3.5. Помимо лиц, указанных в п. 3.4. настоящего Положения, право доступа к персональным данным работников имеют лица, уполномоченные действующим законодательством.

3.6. Лица, имеющие доступ к персональным данным обязаны использовать персональные данные работников лишь в целях, для которых они были предоставлены.

3.7. Ответственным за организацию и осуществление хранения персональных данных работников организации является заместитель директора, в соответствии с приказом директора техникума.

3.8. Персональные данные работника отражаются в личной карточке работника (форма Т-2), которая заполняется после издания приказа о его приеме на работу. Личные карточки работников хранятся в специально оборудованных негорюемых шкафах в алфавитном порядке.

4. Передача персональных данных

4.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

4.1.1. 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 других случаях, предусмотренных Трудовым Кодексом или иными федеральными законами.

4.1.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия.

The first part of the document discusses the importance of maintaining accurate records of all transactions. It emphasizes that proper record-keeping is essential for the integrity of the financial system and for the ability to detect and prevent fraud. The text also mentions the need for regular audits and the role of the auditor in ensuring that the records are reliable.

The second part of the document focuses on the internal controls of the organization. It describes the various measures that should be in place to safeguard assets and ensure the accuracy of financial reporting. This includes the separation of duties, the use of physical controls, and the implementation of a strong internal control system.

The third part of the document discusses the external controls of the organization. It describes the various measures that should be in place to ensure that the organization is compliant with all applicable laws and regulations. This includes the implementation of a strong external control system and the use of external auditors to provide an independent opinion on the financial statements.

The fourth part of the document discusses the role of the auditor in the financial reporting process. It describes the various responsibilities of the auditor, including the need to provide an independent opinion on the financial statements and to detect and prevent fraud. The text also mentions the importance of the auditor's report and the role of the auditor in ensuring the integrity of the financial system.

The fifth part of the document discusses the various factors that can affect the reliability of financial statements. It describes the various risks that are associated with financial reporting and the need for the auditor to be aware of these risks. The text also mentions the importance of the auditor's judgment and the role of the auditor in ensuring the reliability of the financial statements.

The sixth part of the document discusses the various factors that can affect the integrity of the financial system. It describes the various risks that are associated with financial reporting and the need for the auditor to be aware of these risks. The text also mentions the importance of the auditor's judgment and the role of the auditor in ensuring the integrity of the financial system.

4.1.3. 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. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном Трудовым Кодексом и иными федеральными законами.

4.1.4. Осуществлять передачу персональных данных работника в пределах техникума в соответствии с данным Положением, с которым работник должен быть ознакомлен под роспись.

4.1.5. 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.

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 и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

5. Права работника в целях обеспечения защиты персональных данных, хранящихся у работодателя

5.1. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право:

5.1.1. Получать полную информацию о своих персональных данных и их обработке.

5.1.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральными законами. Получение указанной информации о своих персональных данных возможно при личном обращении работника, – к заместителю директора, ответственному за организацию и осуществление хранения персональных данных работников.

5.1.3. На определение своих представителей для защиты своих персональных данных.

5.1.4. На доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору.

5.1.5. Требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства. Указанное требование должно быть оформлено письменным заявлением работника на имя директора техникума. При отказе руководителя организации исключить или исправить персональные данные работника, работник имеет право заявить в письменном виде руководителю организации, осуществляющей образовательную деятельность, о своем несогласии, с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения.

5.1.6. Требовать об извещении организацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.1.7. Обжаловать в суде любые неправомерные действия или бездействия организации при обработке и защите его персональных данных.

6. Обязанности субъекта персональных данных по обеспечению достоверности его персональных данных

6.1. В целях обеспечения достоверности персональных данных работники обязаны:

6.1.1. При приеме на работу в организацию, осуществляющую образовательную деятельность, представлять уполномоченным работникам достоверные сведения о себе в порядке и объеме, предусмотренном законодательством Российской Федерации.

6.1.2. В случае изменения персональных данных работника: фамилия, имя, отчество, адрес места жительства, паспортные данные, сведения об образовании, состоянии здоровья (вследствие выявления в соответствии с медицинским заключением противопоказаний для выполнения работником его должностных, трудовых обязанностей и т.п.) сообщать об этом в течение 5 рабочих дней с даты их изменений.

7. Уничтожение персональных данных

7.1. В соответствии с Приказом Роскомнадзора №179 от 28 октября 2022 года, определены требования к документальному оформлению факта уничтожения персональных данных работников техникуме:

- в случае если обработка персональных данных осуществляется оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных;
- в случае если обработка персональных данных осуществляется оператором с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала).

7.2. Акт об уничтожении персональных данных должен содержать:

- наименование техникуме или фамилию, имя, отчество (при наличии) оператора персональных данных и его адрес;
- наименование техникуме или фамилию, имя, отчество (при наличии) лица, осуществляющего обработку персональных данных субъекта персональных данных по поручению оператора (если обработка была поручена такому лицу);
- фамилию, имя, отчество (при наличии) субъекта или иную информацию, относящуюся к определенному физическому лицу, чьи персональные данные были уничтожены;
- фамилию, имя, отчество (при наличии), должность лиц, уничтоживших персональные данные субъекта персональных данных, а также их подпись;
- перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;
- наименование уничтоженного материального носителя, содержащего персональные данные субъекта персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);
- наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации);
- способ уничтожения персональных данных;
- причину уничтожения персональных данных;
- дату уничтожения персональных данных субъекта (субъектов) персональных данных.

Форма акта об уничтожении персональных данных составляется в произвольной форме.

7.3. Акт об уничтожении персональных данных может быть оформлен как на бумаге, так и в электронной форме. В первом случае он заверяется личной подписью лиц, уничтоживших персональные данные, а во втором – их электронной подписью.

7.4. Выгрузка из журнала должна содержать:

- фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному физическому лицу, чьи персональные данные были уничтожены;
- перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;
- наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных;
- причину уничтожения персональных данных;
- дату уничтожения персональных данных субъекта (субъектов) персональных данных.

7.5. При невозможности указать в выгрузке из журнала какие-либо сведения, их следует отразить в акте об уничтожении персональных данных.

7.6. Если оператор обрабатывает персональные данные, используя и не используя средства автоматизации, при их уничтожении следует оформлять акт об уничтожении и выгрузку из журнала.

7.7. Акт об уничтожении персональных данных и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения персональных данных.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

8.1. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

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

8.3. 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.

8.4. За нарушение правил хранения и использования персональных данных, повлекшее за собой материальный ущерб работодателю, работник несет материальную ответственность в соответствии с действующим трудовым законодательством.

8.5. Материальный ущерб, нанесенный субъекту персональных данных за счет ненадлежащего хранения и использования персональных данных, подлежит возмещению в порядке, установленном действующим законодательством.

8.6. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом № 152-ФЗ «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

8.7. Организация вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных лишь обработку следующих персональных данных:

- относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения (работникам);
- полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных;

данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

- являющихся общедоступными персональными данными;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональных данных на территорию организации или в иных аналогичных целях;
- включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Во всех остальных случаях оператор (руководитель организации, осуществляющей образовательную деятельность, и (или) уполномоченные им лица) обязан направить в уполномоченный орган по защите прав субъектов персональных данных соответствующее уведомление.

9. Заключительные положения

9.1. Настоящее Положение о защите персональных данных работников является локальным нормативным актом, принимается на Общем собрании работников техникума и утверждается (либо вводится в действие) приказом директора организации, осуществляющей образовательную деятельность.

9.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации.

9.3. Положение о защите персональных данных работников техникума принимается на неопределенный срок. Изменения и дополнения к Положению принимаются в порядке, предусмотренном п.9.1. настоящего Положения.

9.4. После принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.

