Муниципальное бюджетное учреждение дополнительного образования
«Детская школа искусств № 68»
МБУДО «ДШИ № 68»

УТВЕРЖДАЮ:
Директор
МБУДО «ДШИ № 68»
_____ Ащеулова Е.В.
11.11.2022.

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В МУНИЦИПАЛЬНОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ «ДЕТСКАЯ ШКОЛА ИСКУССТВ № 68»

(новая редакция)

1. Общие положения

1.1. Положение об обработке персональных данных в Муниципальном бюджетном учреждении дополнительного образования «Детская школа искусств № 68» – локальный нормативный акт (далее – положение), который устанавливает правила обработки персональных данных, требования к защите персональных данных при их обработке в информационных системах персональных данных и без использования средств автоматизации.

1.2. Обработка персональных данных в Муниципальном бюджетном учреждении дополнительного образования «Детская школа искусств № 68» выполняется с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных субъектов, персональные данные которых обрабатываются в учреждении.

1.3. Муниципальное бюджетное учреждение дополнительного образования «Детская школа искусств № 68» в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее-Федеральный закон) является оператором, осуществляющим обработку персональных данных, а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (далее – оператор персональных данных).

1.4. Субъект персональных данных – физическое лицо, личность которого можно прямо или косвенно определить с помощью информации о нем.

1.5. Право оператора на обработку персональных данных субъекта персональных данных ограничивается установленными в ч. 1 ст. 24 Конституции РФ гарантиями защиты прав и свобод граждан, а также требованиями, содержащимися в ТК РФ, ФЗ "О персональных данных", ФЗ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 г. N 149-ФЗ (СЗ РФ. 2006. N 31 (ч. I). Ст. 3448) и в иных федеральных законах.

2. Правила обработки персональных данных

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

обработка персональных данных субъекта может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия субъекту персональных данных в трудоустройстве, получении образования, продвижении по службе, обеспечения личной безопасности субъекта персональных данных, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

при определении объема и содержания обрабатываемых персональных данных субъекта, оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами;

все персональные данные субъекта следует получать у него самого. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Оператор должен сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта персональных данных дать письменное согласие на их получение;

оператор не имеет права получать и обрабатывать сведения о субъекте персональных данных, относящиеся в соответствии с законодательством Российской Федерации в области персональных данных к специальным категориям персональных данных, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации и другими федеральными законами;

оператор не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;

при принятии решений, затрагивающих интересы субъекта персональных данных, оператор не имеет права основываться на персональных данных субъекта персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения;

защита персональных данных субъекта персональных данных от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами;

субъект персональных данных и его представители должны быть ознакомлены под роспись с документами оператора, устанавливающими порядок обработки персональных данных субъекта персональных данных, а также об их правах и обязанностях в этой области;

субъект персональных данных не должен отказываться от своих прав на сохранение и защиту тайны;

оператор, субъект персональных данных и его представители должны совместно вырабатывать меры защиты персональных данных субъекта персональных данных.

2.2. В целях обеспечения защиты персональных данных, хранящихся у оператора, субъекты персональных данных имеют право на:

полную информацию об их персональных данных и обработке этих данных;

свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта персональных данных, за исключением случаев, предусмотренных федеральными законами;

определение своих представителей для защиты своих персональных данных;
требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ или иного федерального закона. При отказе оператора исключить или исправить персональные данные субъекта персональных данных, он имеет право заявить в письменной форме оператору о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера субъект персональных данных имеет право дополнить заявлением, выражающим его собственную точку зрения;
требование об извещении оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта персональных данных, обо всех произведенных в них исключениях, исправлениях или дополнениях;
обжалование в суд любых неправомерных действий или бездействия оператора при обработке и защите его персональных данных.

2.3. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам, в частности, относятся:
1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;
2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на операторов не предусмотренные законодательством Российской Федерации полномочия и обязанности;
3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона;
4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;
6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2.4. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

2.5. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

2.6. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

2.7. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

2.8. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

2.9. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

2.10. В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор обязан в срок, не превышающий десяти рабочих дней с даты получения оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

2.11. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 2.6-2.10, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

2.12. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели хранения персональных данных, если срок хранения персональных данных не установлен законодательством Российской Федерации.

2.13. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки персональных данных или в случае

утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

2.14. При передаче персональных данных субъекта персональных данных работодатель должен соблюдать следующие требования:

не сообщать персональные данные субъекта персональных данных третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в других случаях, предусмотренных ТК РФ или иными федеральными законами;

не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;

предупредить лиц, получающих персональные данные субъекта персональных данных, 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 субъекта персональных данных, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными субъекта персональных данных в порядке, установленном ТК РФ и иными федеральными законами;

осуществлять передачу персональных данных субъекта персональных данных в пределах одной организации, в соответствии с локальными нормативными актами, с которыми субъекта персональных данных должен быть ознакомлен под роспись;

разрешать доступ к персональным данным субъекта персональных данных только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъекта персональных данных, которые необходимы для выполнения конкретных функций;

не запрашивать информацию о состоянии здоровья субъекта персональных данных, за исключением тех сведений, которые относятся к вопросу о возможности выполнения субъектом персональных данных трудовой функции;

передавать персональные данные субъекта персональных данных представителям субъекта персональных данных в порядке, установленном ТК РФ и иными федеральными законами, и ограничивать эту информацию только теми персональными данными субъекта персональных данных, которые необходимы для выполнения указанными представителями их функций.

3. Обработка персональных данных в информационных системах

3.1. Обработка персональных данных в информационных системах (далее – информационные системы персональных данных) осуществляется в соответствии с постановлением Правительства Российской Федерации от 01.11. 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.2. Обеспечение безопасности персональных данных в информационных системах персональных данных достигается путем:

определения угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

применения прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем персональных данных;
учета машинных носителей персональных данных;
обнаружения фактов несанкционированного доступа к персональным данным и принятием мер по прекращению несанкционированного доступа;
восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
установления правил доступа (пароль, логин и др.) к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных.

3.3. Сотрудники оператора, имеющие доступ к информационным системам персональных данных на основании приказа директора, руководствуются инструкцией пользователя информационной системы персональных данных (Приложение 1).

3.4. Сотрудники оператора, имеющие доступ к информационным системам персональных данных, обязаны:
принимать меры, исключающие несанкционированный доступ к используемым программно-техническим средствам;
вести учет электронных носителей информации, содержащих персональные данные, и осуществлять их хранение в металлических шкафах или сейфах;
производить запись персональных данных (отдельных файлов, баз данных) на электронные носители только в случаях, регламентированных порядком работы с персональными данными;
соблюдать установленный порядок и правила доступа в информационные системы, не допускать передачу персональных кодов и паролей к информационным системам персональных данных;
принимать все необходимые меры к надежной сохранности кодов и паролей доступа к информационным системам персональных данных;
работать с информационными системами персональных данных в объеме своих полномочий, не допускать их превышения;
обладать навыками работы с антивирусными программами в объеме, необходимом для выполнения функциональных обязанностей и требований по защите информации.

3.5. При работе сотрудников оператора в информационных системах персональных данных запрещается:
записывать значения кодов и паролей доступа к информационным системам персональных данных;
передавать коды и пароли доступа к информационным системам персональных данных другим лицам;
пользоваться в работе кодами и паролями других пользователей доступа к информационным системам персональных данных;
производить подбор кодов и паролей доступа к информационным системам персональных данных других пользователей;
записывать на электронные носители с персональными данными посторонние программы и данные;
копировать информацию с персональными данными на неучтенные электронные носители информации;
выносить электронные носители с персональными данными за пределы территории оператора;
покидать рабочее место с включенным персональным компьютером без применения аппаратных или программных средств блокирования, доступа к персональному компьютеру;

приносить, самостоятельно устанавливать и эксплуатировать на персональном компьютере любые программные продукты, не принятые к эксплуатации;
открывать, разбирать, ремонтировать персональные компьютеры, вносить изменения в конструкцию, подключать нештатные блоки и устройства;
передавать информацию, содержащую персональные данные, подлежащие защите, по открытым каналам связи (факсимильная связь, электронная почта и иное), а также использовать сведения, содержащие персональные данные, подлежащие защите, в открытой переписке и при ведении переговоров по телефону.

4. Обработка персональных данных без использования средств автоматизации

4.1. Сбор, систематизацию, накопление, хранение, обновление, изменение, передачу, уничтожение (далее – обработка) документов, содержащих персональные данные на бумажном носителе, осуществляют сотрудники оператора в соответствии с гл.14 Трудового Кодекса Российской Федерации.

4.2. Документы, содержащие персональные данные, уничтожаются путем измельчения в бумагорезательной машине или сжигании.

4.3. При смене сотрудника, ответственного за учет документов на бумажном носителе, содержащих персональные данные, составляется акт приема-сдачи этих материалов, который утверждается директором.

4.4. При работе с документами на бумажном носителе, содержащими персональные данные, уполномоченные на обработку персональных данных сотрудники оператора обязаны:
ознакомиться только с теми документами, содержащими персональные данные, к которым получен доступ в соответствии со служебной необходимостью;
хранить в тайне ставшие известными им сведения, содержащие персональные данные, подлежащие защите, информировать непосредственного руководителя о фактах нарушения порядка работы с персональными данными и о попытках несанкционированного доступа к ним;
о допущенных нарушениях установленного порядка работы, учета и хранения документов, содержащих персональные данные, а также о фактах разглашения сведений, содержащих персональные данные, подлежащих защите,
представлять непосредственным руководителям письменные объяснения.

4.5. Сотрудники, виновные в разглашении или утрате информации, содержащей персональные данные, несут ответственность в соответствии с законодательством Российской Федерации.

4.6. Контроль за исполнением сотрудниками оператора требований положения возлагается на ответственного за организацию обработки персональных данных, назначенным приказом директора.

5. Заключительные положения

5.1. Настоящее положение утверждаются директором учреждения на неопределенный срок.

5.2. Изменения и дополнения к положению принимаются в составе новой редакции. После принятия новой редакции положения, предыдущая редакция утрачивает силу.

Приложение 1
к Положению об обработке персональных данных в Муниципальном бюджетном учреждении дополнительного образования «Детская школа искусств № 68»

ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. С целью автоматизации процессов, в Муниципальном бюджетном учреждении дополнительного образования «Детская школа искусств № 68» (далее – учреждение) введена в действие информационная система персональных данных (далее – ИСПДн).

1.2. К работе с компонентами ИСПДн допущены сотрудники (далее – пользователи) на основании приказа, который издается директором учреждения. С целью обеспечения ответственности за нормальное функционирование и контроль работы средств защиты информации в ИСПДн директором назначается ответственный за обеспечение безопасности персональных данных; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности назначается ответственный за организацию обработки персональных данных.

1.3. С целью защиты информации от несанкционированного нарушения ее конфиденциальности, целостности и доступности в ИСПДн организационными и техническими средствами реализована система защиты информации.

1.4. Несмотря на то, что многие действия по защите информации производятся прозрачно для пользователя, он остается активным участником процесса по защите конфиденциальной информации и является вовлеченным в процессы обеспечения информационной безопасности в учреждении.

1.5. Каждому пользователю предоставляется минимально необходимый для выполнения своих служебных обязанностей доступ к ресурсам ИСПДн.

1.6. Пользователи ИСПДн при работе с техническими средствами и информационными технологиями, являющимися частью ИСПДн должны соблюдать положения настоящей Инструкции.

1.7. Настоящая инструкция разработана с учетом положений следующих законодательных и нормативно-правовых актов:

- Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
- Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;
- методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;

2. Общие обязанности пользователя по защите информации в ИСПДн

2.1. Пользователь в ИСПДн выполняет только те действия, которые необходимы для выполнения его служебных обязанностей. Любые посторонние действия в ИСПДн запрещены.

2.2. Пользователь подписывает соглашение о неразглашении конфиденциальной информации перед началом выполнения служебных обязанностей, связанных с доступом к такой информации.

2.3. Пользователь незамедлительно оповещает ответственного за организацию обработки персональных данных о любой подозрительной активности в ИСПДн.

2.4. Пользователю запрещено использовать личные технические средства (ноутбуки, смартфоны, планшеты, фотокамеры, флеш-носители, съемные жесткие диски и пр.) для несанкционированного копирования, фотографирования, распространения и передачи защищаемой информации.

2.5. Пользователь принимает участие в инструктажах по информационной безопасности, проводимый ответственным за обеспечение безопасности персональных данных и/или ответственным за организацию обработки персональных данных. При получении дополнительных материалов от ответственного за обеспечение безопасности персональных данных и/или ответственного за организацию обработки персональных данных во время инструктажей, пользователь самостоятельно изучает их с целью повышения своей осведомленности в вопросах информационной безопасности и защиты персональных данных.

2.6. Пользователь визуально контролирует целостность технических средств на своем рабочем месте (отсутствие попыток физического вскрытия системного блока и пр.). При подозрении на нарушение целостности технических средств ИСПДн, пользователь сообщает об этом ответственному за обеспечение безопасности персональных данных и/или ответственному за организацию обработки персональных данных. Пользователю запрещен самостоятельный ремонт технических средств ИСПДн, а также привлечение посторонних лиц для такого ремонта.

2.7. В случае объективной необходимости, пользователь участвует в составе группы реагирования на инциденты информационной безопасности в расследованиях причин инцидентов безопасности.

2.8. В целях блокирования возможности несанкционированного ознакомления с защищаемой информацией на экране монитора, пользователь должен блокировать сеанс работы в ИСПДн при покидании рабочего места более чем на 2 минуты.

2.9. Пользователю запрещены любые действия в ИСПДн до прохождения процедуры идентификации и аутентификации в системе (до ввода логина и пароля).

2.10. Пользователю запрещено изменение источника загрузки своего автоматизированного рабочего места (далее - АРМ) и загрузка АРМ с внешних носителей.

2.11. Антивирусная защита в ИСПДн реализована прозрачно для пользователя, установка антивирусных программ, обновление антивирусных баз, запуск антивирусных проверок, сбор информации о найденных вирусах производится ответственным за обеспечение безопасности персональных данных централизованно. Пользователю запрещено изменять настройки антивирусного программного обеспечения или отключать его (даже на короткое время). Пользователь должен оповещать ответственного за обеспечение безопасности персональных данных о локальных сообщениях антивирусного программного обеспечения на его АРМ. Пользователь должен оповещать ответственного за обеспечение безопасности персональных данных о любых аномалиях в работе АРМ.

2.12. Пользователю запрещается самостоятельная установка любого программного обеспечения, даже необходимого для выполнения своих служебных обязанностей. Установка разрешенного в ИСПДн программного обеспечения осуществляется

ответственным за обеспечение безопасности персональных данных. Также к установке и настройке программного обеспечения в ИСПДн, при условии соблюдения мер по защите информации, допускаются сотрудники сторонних организаций.

2.13. Пользователь должен пресекать попытки посторонних лиц (или лиц, не имеющих соответствующих полномочий) тем или иным образом получить доступ к его учетным данным, конфиденциальной информации в ИСПДн и к любой другой защищаемой информации. Пользователь незамедлительно сообщает ответственному за обеспечение безопасности персональных данных и/или ответственному за организацию обработки персональных данных о подобных попытках (как удачных, так и неудачных).

2.14. Пользователь в меру своих сил и возможностей содействует проведению служебных расследований, инициированных в связи с инцидентами информационной безопасности.

2.15. Пользователь работает только с теми сетевыми ресурсами (сетевые папки, веб сайты и пр.), которые разрешены и, работа с которыми необходима пользователю для выполнения своих служебных обязанностей.

2.16. Пользователь принимает меры по противодействию несанкционированному просмотру защищаемой информации с экрана монитора посторонними лицами. К таким мерам относятся:

- сворачивание окна, в котором отображена защищаемая информация или блокирование сеанса пользователя при нахождении посторонних лиц вблизи рабочего места пользователя с фронтальной стороны монитора;
- ориентация монитора задней частью к дверным проемам и окнам;
- в случае вынужденной ориентации монитора фронтальной частью к окну, пользователь во время работы с защищаемой информацией закрывает шторы, жалюзи.

2.17. Пользователь должен знать и соблюдать положения настоящей Инструкции, а также других внутренних локальных нормативных документов учреждения. При возникновении у пользователя вопросов по защите информации и защите персональных данных в учреждении, он обращается к ответственному за обеспечение безопасности персональных данных и/или ответственному за организацию обработки персональных данных. Новые пользователи ИСПДн перед началом выполнения своих служебных обязанностей изучают положения настоящей Инструкции.

3. Правила управления идентификаторами, учетными записями и паролями

3.1. Внутренними локальными нормативными документами, определяющими правила управления идентификаторами, учетными записями и паролями являются:

- Положение о Политике Муниципального бюджетного учреждением дополнительного образования «Детская школа искусств № 68» в отношении обработки персональных данных;
- Должностная инструкция ответственного за обработку персональных данных в Муниципальном бюджетном учреждении дополнительного образования «Детская школа искусств № 68»;
- Должностная инструкция ответственного за обеспечение безопасности персональных данных в Муниципальном бюджетном учреждении дополнительного образования «Детская школа искусств № 68»;
- Положение об организации и проведении работ в Муниципальном бюджетном учреждении дополнительного образования «Детская школа искусств № 68» по обеспечению безопасности персональных данных обрабатываемых в информационных системах персональных данных и/или без использования средств автоматизации
- Положение об обработке персональных данных в Муниципальном бюджетном учреждении дополнительного образования «Детская школа искусств № 68», инструкция пользователя ИСПДн.

3.2. Пользователь перед началом работы в ИСПДн получает учетные данные (персональный идентификатор, логин, временный пароль) у ответственного за обеспечение безопасности персональных данных.

3.3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями объекта вычислительной техники самостоятельно с учетом следующих требований:

- пароль должен быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы;
- символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущих;
- пользователь не имеет права сообщать личный пароль другим лицам.

3.4. Пользователю запрещено записывать и хранить пароли в местах, доступных для просмотра посторонним лицам (на отдельных листах бумаги, в не запираемой тумбе, под клавиатурой, на мониторе и т. п.).

3.5. Пользователь должен удостовериться, что при вводе пароля никто не наблюдает за процессом ввода пароля.

3.6. Пользователю запрещено вводить свои учетные данные для предоставления возможности временной работы в ИСПДн другим пользователям или посторонним лицам, поскольку все выполненные этими лицами действия в ИСПДн будут считаться действиями, выполненными пользователем. Ответственность за неправомерные действия таких посторонних лиц несет пользователь.

3.7. Пользователю запрещено оставлять без присмотра персональный идентификатор (электронный ключ).

3.8. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 90 дней.

3.9. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться ответственным за обеспечение безопасности персональных данных, немедленно после окончания последнего сеанса работы данного пользователя с системой.

3.10. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) ответственным за обеспечение безопасности персональных данных.

3.11. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по восстановлению парольной защиты.

3.12. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на ответственного за обеспечение безопасности персональных данных.

4. Работа со съемными носителями информации

4.1. Пользователю разрешается использовать только учтенные съемные носители информации в ИСПДн (флэшки, съемные жесткие диски, карты памяти и пр.).

4.2. При необходимости использования для исполнения служебных обязанностей съемных носителей информации пользователь в письменной форме делает запрос ответственному за обеспечение безопасности персональных данных и/или ответственному за организацию обработки персональных данных на выдачу учтенного съемного носителя информации. Пользователь расписывается за получение и сдачу учтенного съемного носителя информации в Журнале учета носителей информации.

4.3. В случае утери, кражи или компрометации учтенного носителя, пользователь оперативно сообщает об этом ответственному за обеспечение безопасности персональных данных и/или ответственному за организацию обработки персональных данных.

4.4. Пользователь несет ответственность за сохранность выданных ему съемных носителей информации и за конфиденциальность защищаемой информации, записанной на него.