

РАССМОТРЕНО
на педагогическом совете школы
(Протокол от 22.02.2018 № 3)

УТВЕРЖДЕНО
Приказом директора МБОУДО «ДМШ»
от «30» января 2018 г. № 18



Положение
о порядке обработки персональных данных
в муниципальном бюджетном образовательном учреждении
дополнительного образования «Детская музыкальная школа»
(далее – МБОУДО «ДМШ»)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» иными нормативными правовыми актами Российской Федерации, Уставом МБОУДО «ДМШ», иными локальными нормативными документами МБОУДО «ДМШ» (далее - учреждение).

1.2. Настоящее положение устанавливает в учреждении порядок работы с документами – носителями конфиденциальной информации, содержащей персональные данные, в целях:

- предотвращения неконтролируемого распространения конфиденциальной информации, содержащей персональные данные в результате ее разглашения должностным лицом, имеющим доступ к информации, содержащей персональные данные, или получения несанкционированного доступа к конфиденциальной информации;
- предотвращения несанкционированного уничтожения, искажения, копирования, блокирования информации, содержащей персональные данные;
- предотвращения утраты, несанкционированного уничтожения или сбоя в процессе функционирования автоматизированных систем обработки информации, содержащей персональные данные, обеспечение полноты, целостности, достоверности такой информации;
- соблюдения правового режима использования информации, содержащей персональные данные;
- обеспечения возможности обработки и использования персональных данных учреждением, его структурными подразделениями и должностными лицами, имеющими соответствующие полномочия.

1.3. Обработка персональных данных осуществляется учреждением с согласия субъекта персональных данных.

Согласие субъекта на обработку его персональных данных не требуется в следующих случаях:

- если персональные данные являются общедоступными;
- когда персональные данные относятся к состоянию здоровья субъекта и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных

интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, а получение согласия субъекта невозможно;

- если обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработки персональных данных по требованию уполномоченных на то государственных органов в случаях, предусмотренных федеральным законом;
- когда обработка персональных данных осуществляется в целях исполнения обращения, запроса самого субъекта персональных данных, трудового или иного договора с ним.

1.4. В целях обеспечения сохранности и конфиденциальности информации, содержащей персональные данные, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться работниками учреждения, осуществляющими данную работу в соответствии с перечнем работников, имеющих доступ к персональным данным.

1.5. Режим конфиденциальности персональных данных отменяется в случаях обезличивания этих данных, в отношении персональных данных, ставших общедоступными, или по истечении 75-летнего срока их хранения, если иное не предусмотрено законом.

1.6. В структурных подразделениях учреждения, имеющих доступ к информации, содержащей персональные данные, формируются и ведутся перечни персональных данных с указанием регламентирующих документов, мест хранения и лиц, ответственных за хранение и обработку данных.

1.7. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, не допускается.

2. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых без использования средств автоматизации

2.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна вестись таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных.

2.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе лица, осуществляющие такую обработку по договору с учреждением), должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

2.4. Материальные носители с персональными данными должны храниться в запирающихся на ключ помещениях, металлических шкафах, сейфах, иных шкафах, имеющих запираемые блок-секции.

2.5. Должностным лицам, работающим с персональными данными, запрещается разглашать информацию, содержащую персональные данные, устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью.

2.6. Не допускается без согласования с руководителем учреждения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих персональные данные.

2.7. Передача персональных данных допускается только в случаях, установленных законодательством Российской Федерации и действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению вышестоящих должностных лиц.

2.8. Передача персональных данных не допускается с использованием средств телекоммуникационных каналов связи (телефон, телефакс, электронная почта и т.п.) без письменного согласия субъекта персональных данных, за исключением случаев, установленных законодательством Российской Федерации.

2.9. После подготовки и передачи документа файлы, копии, черновики документа «переносятся» подготовившим их должностным лицом на маркированные носители, предназначенные для хранения персональных данных.

2.10. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах запроса или опубликованных в общедоступных источниках.

2.11. В учреждении обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающие одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

2.12. При использовании типовых форм документов, характер информации которых предполагает или допускает включение в них персональных данных (далее типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых учреждением способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своей согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

2.12. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию учреждения, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальным актом учреждения, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию учреждения без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию учреждения.

2.13. Работники структурных подразделений в работе должны руководствоваться формой Журнала учета обращений субъектов персональных данных об ознакомлении с их персональными данными в учреждении.

Для ведения Журнала учета обращений субъектов персональных данных об ознакомлении с их персональными данными в структурном подразделении назначаются лица, ответственные за ведение и хранение Журнала учета обращений субъектов персональных данных об ознакомлении с их персональными данными.

Журнал учета обращений субъектов персональных данных об ознакомлении с их персональными данными должен быть пронумерован, прошнурован и скреплен подписью руководителя структурного подразделения.

Хранение Журнала учета обращений субъектов персональных данных об ознакомлении с их персональными данными должно исключать несанкционированный доступ к нему.

2.14. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.15. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, но с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

2.16. Лица, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под расписку с настоящим Положением.

2.17. Лица, осуществляющие обработку и (или) хранение персональных данных в учреждении, несут ответственность за обеспечение их информационной безопасности. Лица, виновные в нарушении норм, регулирующих обработку и хранение персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

3. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых с использованием средств автоматизации

3.1. Безопасность персональных данных при их обработке в автоматизированных информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

3.2. Допуск должностных лиц к обработке персональных данных в автоматизированной информационной системе осуществляется на основании соответствующих разрешительных документов и ключей доступа (паролей).

3.3. Размещение автоматизированных информационных систем, специальное оборудование и организация с их использованием работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в соответствующих помещениях посторонних лиц.

3.4. Компьютеры и(или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа или под чужими, а равно общими (одинаковыми) паролями, не допускается.

3.5. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, не допускается.

3.6. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

3.7. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

- недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3.8. При обработке персональных данных в автоматизированной информационной системе разработчиками и администраторами систем должны обеспечиваться:

- обучение лиц, использующих средства защиты информации, применяемые в автоматизированных информационных системах, правилами работы с ними;

- учет лиц, допущенных к работе с персональными данными в автоматизированной информационной системе, прав и паролей доступа;

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- описание системы защиты персональных данных;

- иные требования по защите персональных данных, установленных инструкциями учреждения по их использованию и эксплуатации.

3.9. Особенности обеспечения безопасности информации и конфиденциальности персональных данных, связанные с использованием конкретных автоматизированных информационных систем, определяются локальными нормативными документами учреждения, регламентирующими порядок использования указанных информационных систем, а также эксплуатационной и инструктивной документацией, касающейся технических средств обработки персональных данных в рамках конкретной автоматизированной информационной системы.

4. Порядок учета, хранения и обращения со съемными носителями персональных данных (их твердыми копиями), а также их утилизации

4.1. Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.2. Учет и выдачу съемных носителей персональных данных по утвержденной форме осуществляют работники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Работники учреждения получают учетный съемный носитель персональных данных от уполномоченного лица для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному должностному лицу, о чем делается соответствующая запись в журнале учета.

4.3. Не допускается:

- хранение съемных носителей с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставление их без присмотра или передача на хранение другим лицам;

- вынос съемных носителей с персональными данными из служебных помещений для работы с ними вне учреждения.

4.4. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов имеющих гриф «ДСП» (для служебного пользования). Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя учреждения.

4.5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся на них сведений немедленно ставится в известность руководитель учреждения.

На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей персональных данных.

4.6. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется соответствующей комиссией, состав которой утверждается приказом руководителя учреждения. По результатам уничтожения носителей составляется акт утвержденной формы.