ЧАСТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ДЕТСКИЙ САД № 206 ОТКРЫТОГО АКЦИОНЕРНОГО ОБЩЕСТВА «РОССИЙСКИЕ ЖЕЛЕЗНЫЕ ДОРОГИ»

Согласовано с ППО
Детского сада № 206 ОАО «РЖД»
Протокол от 29.12.2018 г.
Председатель ППО И.В. Тупицина

УТВЕРЖДЕНО
Приказом заведующего
Детским садом № 206 ОАО «РЖД»
О.А. Дембовской
№ 366-ОД от 29.12.2018 г.

ИНСТРУКЦИЯ
о порядке обеспечения конфиденциальности и безопасности при обращении с информацией, содержащей персональные данные в частном дошкольном образовательном учреждении «Детский сад № 206 открытого акционерного общества «Российские железные дороги»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция разработана 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», постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными правовыми актами Российской Федерации, Уставом Детский сад № 206 ОАО «РЖД» (далее – ДОУ).

1.2. Настоящая Инструкция устанавливает в ДОУ 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 сбоев в процессе функционирования автоматизированных систем обработки информации, содержащей персональные данные, обеспечения полноты, целостности, достоверности такой информации;

– соблюдения правового режима использования информации, содержащей персональные данные;

– обеспечения возможности обработки и использования персональных данных ДОУ должностными лицами, имеющими соответствующие полномочия.

1.3. Обработка персональных данных осуществляется ДОУ 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 работника 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 работника 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;

– обработки адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;

– обработки данных, включающих в себя только фамилии, имена и отчества;

– когда обработка персональных данных осуществляется в целях однократного пропуска на территорию ДОУ или в иных аналогичных целях;

– обработки персональных данных без использования средств автоматизации.

1.4. В целях обеспечения сохранности и конфиденциальности информации, содержащей персональные данные, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться специалистами ДОУ, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

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 нормативно-правовыми актами.

1.6. В ДОУ формируются и ведутся перечни персональных данных работников и воспитанников с указанием мест хранения и лиц, ответственных за хранение и обработку данных. Указанные перечни составляются и утверждаются приказом заведующего.

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, 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 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.

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.

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

2.9. 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.

2.10. В ДОУ 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.

2.11. 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 Университетом способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект

персональных данных может поставить отметку о своем 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 ДОУ, или в иных аналогичных целях, должны соблюдаться следующие условия:

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

б) 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 должны руководствоваться формой Журнала учета обращений субъектов персональных данных об ознакомлении с их персональными данными, установленной Приложением 1 к настоящей Инструкции.

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.

Лица, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под расписку с настоящей Инструкцией.

2.16. Лица, осуществляющие обработку и (или) хранение персональных

данных, 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 несанкционированных 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.

3.9. Особенности обеспечения безопасности информации и конфиденциальности персональных данных, связанные с использованием конкретных автоматизированных информационных систем, определяются Положением об обработке персональных данных ДОУ, регламентирующим 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 уточнения, блокирования и уничтожения персональных данных

4.1. Блокирование информации, содержащей персональные данные работников и воспитанников производится в случае:

– если персональные данные являются неполными, устаревшими, недостоверными;

– если сведения являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

4.2. В случае подтверждения факта недостоверности персональных данных, работники, ответственные за персональные данные в ДОУ, на основании документов, представленных работником, или родителями (законными представителями) воспитанников, уполномоченным органом по защите прав субъектов персональных данных или полученных в ходе самостоятельной проверки, обязаны уточнить персональные данные и снять их блокирование.

4.3. В случае выявления неправомерных действий с персональными данными, ДОУ обязано устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные.

4.4. Уничтожение материального носителя:

– **Бумажный носитель.** Используются 2 вида уничтожения: уничтожение через измельчение и уничтожение через сжигание.

– **Электронный носитель.** Уничтожение заключается в механическом воздействии на рабочие слои дисков, в результате, которого разрушается физическая, магнитная или химическая структура рабочего слоя. Съём данных с магнитных дисков, подвергшихся таким воздействиям, становится невозможным. Факт уничтожения носителей персональных данных оформляется актом (Приложение 2).

Приложение 1
к инструкции о порядке
обеспечения конфиденциальности
и безопасности при обращении с
информацией, содержащей
персональные данные

Журнал
учета обращений субъектов персональных данных об
ознакомлении с их персональными данными

№ п/п	Дата обращения	Сведения о запрашиваемом лице	Краткое содержание обращения	Отметка о предоставлении или отказе в предоставлении информации	Способ предоставления информации	Дата передачи/отказа в предоставлении информации	Подпись ответственного должностного лица	Примечания
1	2	3	4	5	6	7	8	9

Приложение 2
к инструкции о порядке
обеспечения конфиденциальности
и безопасности при обращении с
информацией, содержащей
персональные данные

УТВЕРЖДАЮ
Заведующий
Детским садом № 206 ОАО «РЖД»
_____ /_____/
(подпись) (Ф.И.О.)
«____»_____ 20_____г.

АКТ № _____
об уничтожении съемных носителей / бумажных носителей, персональных данных в Детском саду № 206 ОАО «РЖД»

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела отбор съемных/бумажных носителей персональных данных, не подлежащих дальнейшему хранению

№ п/п	Дата	Наименование съемного/бумажного носителя	Пояснения)

Всего съемных/бумажных носителей _____
(цифрами и прописью)

На съемных/бумажных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены путем:

_____

(разрезания, демонтажа, измельчения, сжигания и т.п.)

Измельчены и сданы для уничтожения предприятию по утилизации вторичного сырья _____

Наименование предприятия по утилизации.

Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/
_____ /_____/