Российская Федерация
муниципальное бюджетное дошкольное образовательное учреждение
«Детский сад № 309» (МБДОУ № 309)
660131, г. Красноярск, ул. Воронова д. 16 Д, тел: 8 (391) 220-26-51, 266-30-90
ОГРН 1022402485775, ИНН 2465047132, КПП 246501001
e-mail: dou309@mailkrsk.ru, веб-сайт: http://kras-dou.ru/309/

ПРИНЯТО: на Общем собрании
трудового коллектива: протокол №03 от 06.04.2022.
СОГЛАСОВАНО: ППО МБДОУ № 309
МБДОУ № 309 _____ Грязева О.Г.
06.04.2022

УТВЕРЖДАЮ:
Заведующий МБДОУ № 309
_____ Новоселова О.М.
Приказ № 84/1 от: 06.04.2022

ИНСТРУКЦИЯ
о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные в МБДОУ № 309

1. Общие положения

1.1. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (далее – 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», Указом Президента Российской Федерации от 06.03.1997 № 188 (с изменениями и дополнениями от 23 сентября 2005 г., 13 июля 2015 г.), постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными правовыми актами Российской Федерации.

1.2. Настоящая Инструкция устанавливает в муниципальном бюджетном дошкольном образовательном учреждении «Детский сад № 309» (далее – учреждение) 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, обеспечение полноты, целостности, достоверности такой информации;
- соблюдения правового режима использования информации, содержащей персональные данные;
- обеспечения возможности обработки и использования персональных данных учреждением и должностными лицами, имеющими соответствующие полномочия.

1.3. Обработка персональных данных осуществляется в учреждении 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;
- обработки адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;
- обработки данных, включающих в себя только фамилии, имена и отчества;
- 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 сотрудниками учреждения, 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 законом.

1.6. В учреждении должностными лицами, имеющими 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.

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.

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 формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих персональные данные.

2.7. Передача персональных данных допускается только в случаях, установленных

действующим 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 действующим законодательством Российской Федерации.
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 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.
2.11. При использовании типовых форм документов, характер информации которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:
- 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 способов обработки персональных данных;
- 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;
- 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;
- 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, должны соблюдаться следующие условия:
- 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 внесении изменений в персональные данные субъекта;
- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза.
2.13. Лица, имеющие отношение к работе с персональными данными, в работе должны руководствоваться формой Журнала учета обращений субъектов персональных данных о выполнении законных прав (Приложение № 1), при обработке персональных данных в учреждении.

Для ведения Журнала учета обращений субъектов персональных данных о выполнении законных прав, при обработке персональных данных в учреждении назначается лицо, ответственное за ведение и хранение Журнала учета обращений субъектов персональных данных о выполнении законных прав. Журнал учета обращений субъектов персональных данных о выполнении законных прав, при обработке персональных данных в Учреждении должен быть пронумерован, прошнурован и скреплен подписью заведующего Учреждением. Хранение Журнала учета обращений субъектов персональных данных о выполнении законных прав, при обработке персональных данных в учреждении должно исключать несанкционированный доступ к нему.
2.14. Для обработки различных категорий персональных данных, осуществляемых 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 настоящей Инструкцией.
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 действующим 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 действующим 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 ответственными лицами должны обеспечиваться:
- непрерывное 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 обеспечением соблюдения условий за использованием 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. Локальные акты регламентируют 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 учѐту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.
4.2. Учет съемных носителей, содержащий персональные данные должен производиться по форме, установленной (Приложением № 2).
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 на дому и т.д.
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 заведующего учреждением.
4.5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся на них сведений немедленно ставится в известность заведующий учреждением. 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 заведующего учреждением. По результатам уничтожения носителей составляется акт по форме, установленной
(Приложением 3).

5. Заключительные положения

5.1. Настоящее Положение вступает в силу с даты его утверждения заведующим (и.о. заведующего) учреждения и действует до принятия нового Положения.
5.2. Дополнения, изменения в Положение вносятся в установленном Уставом порядке: принимаются на общем собрании работников учреждения и утверждаются приказом заведующего (и.о. заведующего) учреждения.

Приложение 1

ЖУРНАЛ
учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных

начат _____
окончен_____

Хранить 75 лет
На ____ листах

№ п/п	Сведения о запрашиваю--щем лице	Содержание обращения	Цель запроса	Отместка о предоставлении информации или отказе в ее предоставлении	Дата передачи /отказа в предоставлении информации	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8

Приложение 2

ЖУРНАЛ
учета приема и передачи ключевого носителя (ЭЦП)

начат _____
окончен_____

Хранить 5 лет
На ____ листах

№ п/п	Тип носителя ЭЦП	Идентификатор ЭЦП	Дата и время передачи носителя	ФИО лица. Принявшего носитель	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7

_____ _____
Должность и ФИО ответственного за хранение Подпись

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными)

Приложение 3

АКТ
уничтожения съемных носителей персональных данных

Комиссия, образованная приказом заведующего от «___» _____ 20____ г. № _____, в составе:
председателя - _____
ФИО, должность
членов - _____
_____
ФИО, должности
провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№	Дата	Учетный номер съемного носителя	Пояснения

Всего съемных носителей_____
(цифрами и прописью)
На съемных 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 и т.п.),
измельчены и сданы для уничтожения предприятию по утилизации вторичного сырья
_____ _____
Наименование предприятия по утилизации Дата
Председатель комиссии _____ / _____/
_____ Подпись Фамилия И.О.
Дата

Члены комиссии:
_____
_____

Российская Федерация
муниципальное бюджетное дошкольное образовательное учреждение
«Детский сад № 309» (МБДОУ № 309)
660131, г. Красноярск, ул. Воронова д. 16 Д, тел: 8 (391) 220-26-51, 266-30-90
ОГРН 1022402485775, ИНН 2465047132, КПП 246501001
e-mail: dou309@mailkrsk.ru, веб-сайт: http://kras-dou.ru/309 /

ПРИНЯТО: на Общем собрании
трудового коллектива: протокол № ___ от _____
СОГЛАСОВАНО: ППО МБДОУ № 309
МБДОУ № 309 _____ Грязева О.Г.

УТВЕРЖДАЮ:
Заведующий МБДОУ № 309
_____ Новоселова О.М.
Приказ № _____ от _____

ПОЛОЖЕНИЕ
о парольной защите при обработке персональных данных и иной конфиденциальной информации в МБДОУ № 309

1. Общие положения

1.1 Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах (ИС) организации, а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями в муниципальном бюджетном дошкольном образовательном учреждении «Детский сад № 309» (далее – учреждение). Парольная защита требует соблюдения ряда правил, изложенных в настоящем Положении.
1.2 Цель - Положение определяет требования учреждения к парольной защите информационных систем.
1.3 Область действия - Положение распространяется на всех пользователей и информационные системы (далее – ИС) учреждения, использующих парольную защиту.

2. Термины и определения

2.1 ИС – в данном случае любая информационная система, для работы с которой необходима аутентификация пользователя.
2.2 Пароль – секретный набор символов, используемый для аутентификации пользователя.
2.3Пользователи – администраторы ИС и работники Общества или сторонней организации, которым предоставлен доступ к ИС Общества, а также корпоративный доступ к ресурсам сети Интернет.
2.4 Учетная запись – идентификатор пользователя, используемый для доступа к ИС.

3. Положения

3.1 Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом следующих требований:
- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры;
- 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 предыдущего не менее чем в 6 позициях;
- личный пароль Пользователь не имеет права сообщать никому.

3.2 Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3.3 При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых сотрудников (Пользователей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей сообщать руководителю их новые значения.

3.4 Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться сотрудниками, отвечающими за работу ИС немедленно после окончания последнего сеанса работы данного Пользователя с системой.

3.5 Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

3.6 Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя в опечатанном конверте.

3.7 Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на сотрудников, имеющих доступ к ИС.

4. Роли и ответственность

4.1Пользователи: Исполняют требования положения и несут ответственность за ее нарушение. Информируют администратора парольной защиты обо всех ставших им известных случаях нарушения настоящего положения.

4.2 Администратор парольной защиты:
- Принимает обращения пользователей по вопросам парольной защиты (например, блокировка четных записей, нарушение положения и др.).
- Организует консультации пользователей по вопросам использования парольной защиты.
- Контролирует действия Пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования.
- Отвечает за безопасное хранение паролей встроенных административных учетных записей.

5. Заключительные положения

5.1. Настоящее Положение вступает в силу с даты его утверждения заведующим (и.о. заведующего) учреждения и действует до принятия нового Положения.

5.2.Дополнения, изменения в Положение вносятся в установленном Уставом порядке: принимаются на общем собрании работников учреждения и утверждаются приказом заведующего (и.о. заведующего) учреждения.

Пронумеровано прошнуровано
10 (десять) листов
Заведующий МБДОУ №309
Новоселова О.М.
Дата: 16.01.2020г.