МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
г. МУРМАНСКА № 104

Номер документа	Дата составления
51/01-15	15.04.2016 г.

ПРИКАЗ

«О порядке обработки и защите
персональных данных в
МБДОУ г. Мурманска № 104»

Согласно Федеральному закону от 23.12.2010 № 359-ФЗ «О внесении изменения в статью 25 Федерального закона "О персональных данных", образовательное учреждение (далее – ОУ) должно привести информационные системы персональных данных в соответствие с требованиями Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее – Закон № 152-ФЗ) в соответствии с вышеизложенным приказываю:

1. Утвердить Положение о защите персональных данных работников в муниципальном бюджетном дошкольном образовательном учреждении г. Мурманска № 104 (в которое включен порядок обработки и защиты персональных данных) с приложением № 1 – формой согласия на обработку персональных данных;

2. Утвердить Положение о защите персональных данных воспитанников и родителей (законных представителей воспитанников) в муниципальном бюджетном дошкольном образовательном учреждении г. Мурманска № 104 (в которое включен порядок обработки и защиты персональных данных) с приложением № 1 – формой согласия на обработку персональных данных, приложением № 2 – формой согласия на обработку персональных данных в АИС «электронный детский сад»;

3. Возложить персональную ответственность за организацию защиты персональных данных сотрудников МБДОУ с 15.04.2016 года на сотрудников, которые при выполнении должностных обязанностей имеют доступ к персональным данным:

4. Возложить персональную ответственность за организацию защиты персональных данных воспитанников и родителей (законных представителей воспитанников) МБДОУ с 15.04.2016 года на сотрудников, которые при выполнении должностных обязанностей имеют доступ к персональным данным:

5. Назначить лицом, ответственным за техническое администрирование организации защиты персональных данных – делопроизводителя Агапову Л.К. с 15.04.2016 года. В ее отсутствие ответственность возлагается на сотрудника, замещающего данную должность по приказу (с ознакомлением с данным приказом и всеми документами по данному приказу), при отсутствии замены - на заведующую МБДОУ – Смирнову Е.С.

6. Утвердить организационно-нормативных документы:

- список работников ДОУ, допущенных к обработке персональных данных (приложение 1 к приказу);

- форма журнала обращений по ознакомлению с персональными данными (приложение 2 к приказу);
- различные формы анкет для воспитанников и их родителей (законных представителей) (приложение 3 к приказу);
- инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (приложение 4 к приказу);
- инструкция пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники (приложение 5 к приказу);
- инструкция по проведению мониторинга информационной безопасности и антивирусного контроля (приложение 6 к приказу);
- инструкция по организации парольной защиты (приложение 7 к приказу).

7. Всем сотрудникам, ответственным за обработку и защиту персональных данных руководствоваться в своей деятельности нормативными документами:

- Федеральный закон от 23.12.2010 № 359-ФЗ «О внесении изменения в статью 25 Федерального закона "О персональных данных"»
- Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" (ред. от 23.12.2010)
- Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (ред. от 06.04.2011)
- Федеральный закон от 02.05.2006 № 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации" (ред. от 27.07.2010)

8. Делопроизводителю Агаповой Л.К. до 21.06.2016 года:
* составить папку с вложением в нее нормативной документацией в соответствии с пунктом 7 данного приказа;
* завести журналы в соответствии с приложением № 1,2.

9. Контроль за выполнением данного приказа оставляю за собой.

Заведующая МБДОУ г. Мурманска № 104 ____ Смирнова Е.С.

Приложение № 1
к приказу № 51 /01-15

Форма списка работников, допущенных к обработке персональных данных

Ф.И.О. работника	Должность	Дата приема на работу	Адрес, телефон	Примечание

Приложение № 2
к приказу №51 /01-15

Форма журнала обращений по ознакомлению с персональными данными

Ф.И.О. работника	Дата обращения	Запрашиваемый документ (данные)	Отметка о выполнении	Подпись заявителя	Примечание

Приложение № 3
к приказу № 51 /01-15

Анкета для родителей (законных представителей)

Ф.И.О.: _____

Дата рождения: _____

Образование: _____

Место работы: _____

Занимаемая должность: _____

Домашний адрес: _____

Домашний телефон: _____

Служебный телефон: _____

E-mail: _____

Дата заполнения: "____" _____ 20 ___ г. Личная подпись _____

Дата размещения: «__»_____ _____г.

Приложение № 3
к приказу № 51 /01-15

Уважаемые родители!

С 1 января 2010 года все организации, осуществляющие обработку персональных данных, должны соответствовать требованиям Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных».

Сейчас в нашем ДОУ собираются, хранятся и обрабатывается персональные данные Ваших детей, поэтому руководителю необходимо сделать все, чтобы было соблюдено действующее законодательство в области защиты персональных данных.

Для этого ДОУ должна получить от родителей каждого ученика согласие на обработку его персональных данных (ПДн). Без такого согласия мы не сможем вести учет Ваших детей в привычном режиме.

Руководство ДОУ гарантирует, в случае получения такого согласия с Вашей стороны, принятие максимального качества мер по защите ПДн Ваших детей в соответствии с требованиями действующего законодательства и нормативных документов регуляторов в области защиты ПДн.

При этом мы прекрасно понимаем, что понятие «общедоступности» может вызвать у Вас некоторую настороженность. Мы гарантируем, что такое согласие будет храниться в ДОУ, его содержание будет недоступно другим и действие согласия будет распространяться только на Наше учреждение. Любой другой оператор ПДн должен будет независимо получать от Вас разрешение на обработку ПДн Ваших детей.

Согласие на обработку и передачу персональных Ваших данных и данных ребенка ребёнка состоит их 2-х документов:

1- согласие на обработку персональных данных

2- согласие на обработку персональных данных в АИС «Электронный детский сад»

С нормативными актами по защите ПДн можно ознакомиться у делопроизводителя или руководителя ДОУ.

Приложение № 4
к приказу № 51 /01-15

Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

1. Общие положения

1.1. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (далее – Инструкция), является обязательной для всех структурных подразделений дошкольного образовательного учреждения (далее – ДОУ).

1.2. Под персональными данными понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в т. ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессия, доходы и др.

1.3. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных, а также в отношении общедоступных персональных данных.

В общедоступные источники персональных данных (в т. ч. справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес и другие сведения.

1.4. Конфиденциальность персональных данных предусматривает обязательное получение согласия субъекта персональных данных (наличие иного законного основания) на их обработку.

Согласие не требуется на обработку данных:

- необходимых для доставки почтовых отправлений организациями почтовой связи;
- включающих в себя только фамилию, имя и отчество субъекта;
- данных, работа с которыми проводится в целях исполнения обращения (запроса) субъекта персональных данных, трудового или иного договора с ним, однократного пропуска в здание или в иных аналогичных целях;
- обработка которых осуществляется без средств автоматизации.

1.5. Порядок ведения перечней персональных данных в структурных подразделениях ДОУ утверждается локальным актом. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.

1.6. Все работники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны иметь допуск (разрешение) к работе с соответствующими видами персональных данных.

1.7. Работникам, осуществляющим обработку персональных данных, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью, а также оставлять материальные носители с персональными данными без присмотра в незапертом помещении. После подготовки и передачи документа в соответствии с резолюцией файлы черновиков и вариантов документа должны переноситься подготовившим их работником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

1.8. Передача персональных данных допускается только в случаях, установленных Федеральными законами от 27.07.2006 № 152-ФЗ "О персональных данных" и от 02.05.2006 № 59-ФЗ "О порядке

рассмотрения обращений граждан Российской Федерации", действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

1.9. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством РФ и действующими инструкциями по работе со служебными документами и обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

1.10. Ответственность за защиту обрабатываемых персональных данных возлагается на работников подразделений ДОУ, осуществляющих такую обработку по договору с оператором, а также на иные лица, осуществляющие обработку или хранение конфиденциальных данных в ДОУ. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную и уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами.

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 быть организована таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения материальных носителей персональных данных и установить перечень лиц, осуществляющих обработку.

2.2. При хранении материальных носителей необходимо соблюдать условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. 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 выполнения такой обработки.

2.3. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается на одном материальном носителе размещать персональные данные, цели обработки которых заведомо не совместимы. Для обработки персональных данных каждой категории должен использоваться отдельный материальный носитель.

2.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, и невозможности обработки одних персональных данных отдельно от других, зафиксированных на том же носителе, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающие одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

2.5. Уничтожение или обезличивание всех или части персональных данных (если это допускается материальным носителем) производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Уточнение персональных данных 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.

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

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

3.2. Допуск лиц к обработке персональных данных в информационных системах осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

3.3. Работа с информационными системами должна быть организована таким образом, чтобы обеспечить сохранность носителей персональных данных и средств защиты информации, а также исключить возможность неконтролируемого пребывания в помещениях, где они находятся, 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 шести и более символов.

3.5. Работа на компьютерах с персональными данными без паролей доступа или под чужими или общими (одинаковыми) паролями, а также пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в т. ч. сети Интернет, запрещается.

3.6. При обработке персональных данных в информационных системах 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 и подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3.7. При обработке персональных данных в информационных системах разработчики и администраторы систем должны обеспечивать:

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет лиц, допущенных к работе с персональными данными в информационных системах, 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.

3.8. Специфические требования к защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

3.9. Работники подразделений ДОУ и лица, выполняющие работы по договорам и контрактам, имеющие отношение к обработке персональных данных, должны быть ознакомлены с Инструкцией под расписку.

Приложение № 5
к приказу № 51 /01-15

Инструкция пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники

1. Общие положения

1.1. Инструкция пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники (далее – Инструкция), регламентирует основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) дошкольного образовательного учреждения (далее – ДОУ).
1.2. Инструкция регламентирует деятельность пользователя, который имеет допуск к обработке соответствующих категорий персональных данных и обладает необходимыми навыками работы на ПЭВМ.

2. Обязанности пользователя

2.1. При выполнении работ в пределах своих функциональных обязанностей пользователь несет персональную ответственность за соблюдение требований нормативных документов по защите информации.
2.2. Пользователь обязан:

- выполнять требования Инструкции по обеспечению режима конфиденциальности проводимых работ;
- при работе с персональными данными исключать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц, а также располагать во время работы экран видеомонитора так, чтобы отображаемая на нем информации была недоступна для просмотра посторонними лицами;
- соблюдать правила работы со средствами защиты информации, а также установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;
- после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня стирать остаточную информацию с жесткого диска ПЭВМ;
- оповещать обслуживающий ПЭВМ персонал, а также непосредственного руководителя обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;
- не допускать "загрязнения" ПЭВМ посторонними программными средствами;
- знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, меры предотвращения ухудшения ситуации;
- знать и соблюдать правила поведения в экстренных ситуациях, порядок действий при ликвидации последствий аварий;
- помнить личные пароли и персональные идентификаторы;
- знать штатные режимы работы программного обеспечения, пути проникновения и распространения компьютерных вирусов;
- при применении внешних носителей информации перед началом работы проводить их проверку на наличие компьютерных вирусов.

2.3. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции. В случае обнаружения зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

2.4. Пользователю ПЭВМ запрещается:

- записывать и хранить персональные данные на неучтенных в установленном порядке машинных носителях информации;
- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;
- самостоятельно подключать к ПЭВМ какие-либо устройства, а также вносить изменения в состав, конфигурацию и размещение ПЭВМ;
- самостоятельно устанавливать и/или запускать на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;
- осуществлять обработку персональных данных в условиях, позволяющих просматривать их лицам, не имеющим к ним допуска, а также нарушающих требования к эксплуатации ПЭВМ;
- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;
- отключать (блокировать) средства защиты информации;
- производить какие-либо изменения в подключении и размещении технических средств;
- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями;
- бесконтрольно оставлять ПЭВМ с загруженными персональными данными, установленными маркированными носителями, электронными ключами и выведенными на печать документами, содержащими персональные данные.

3. Права пользователя

Пользователь ПЭВМ имеет право:

- обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий;
- обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

4. Заключительные положения

4.1. Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

4.2. Работники подразделений ДОУ и лица, выполняющие работы по договорам и контрактам и имеющие отношение к обработке персональных данных на объектах вычислительной техники, должны быть ознакомлены с Инструкцией под расписку.

Приложение № 6
к приказу № 51 /01-15

Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля

1. Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля (далее – Инструкция) регламентирует порядок планирования и проведения мероприятий, направленных на обеспечение безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации, необходимой в работе дошкольного образовательного учреждения (далее – ДОУ).
2. Мониторинг работоспособности аппаратных компонентов автоматизированных систем, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование), должны постоянно контролироваться в рамках работы администраторов соответствующих систем.
3. Мониторинг парольной защиты предусматривает:
   - контроль соблюдения сроков действия паролей (не более трех месяцев);
   - периодическую (не реже одного раза в месяц) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств ("взломщиков" паролей).
4. Мониторинг целостности программного обеспечения включает:
   - проверку контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;
   - сверку дубликатов идентификаторов пользователей;
   - проверку и восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.
5. Мероприятия, направленные на предупреждение и своевременное выявление попыток несанкционированного доступа, в т. ч. выявление фактов сканирования определенного диапазона сетевых портов в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и определяющих места ее уязвимости, осуществляются с использованием средств операционной системы и специальных программных средств. Они должны сопровождаться фиксацией неудачных попыток входа в систему в системном журнале и протоколированием работы сетевых сервисов.
6. Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, осуществляется по обращениям пользователей в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности.
7. Системный аудит производится ежеквартально и в особых ситуациях. Он включает в себя проведение обзоров безопасности, тестирование системы и контроль внесения изменений в системное программное обеспечение.
8. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, уровню безопасности, удовлетворяющему требованиям политики безопасности, и включают:
   - составление отчетов о безопасности пользовательских ресурсов (в т. ч. о наличии повторяющихся пользовательских имен и идентификаторов, неправильных форматах регистрационных записей, пользователях без пароля, неправильной установке домашних каталогов пользователей и уязвимостях пользовательских окружений);
   - проверку содержимого файлов конфигурации на соответствие списку для проверки;
   - анализ данных об обнаружении изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);

- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);
- оценку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;
- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

9. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в информационную систему с помощью автоматического инструментария или вручную.
10. Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Сначала информация об известных уязвимостях извлекается из документации и внешних источников, затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то с целью нейтрализации уязвимостей необходимо выполнить одно из следующих действий:

- изменить конфигурацию системы (для ликвидации условий проявления уязвимости);
- установить программные коррекции либо другие версии программ, в которых данная уязвимость отсутствует;
- отказаться от использования системного сервиса, содержащего данную уязвимость.

11. Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные, с обязательным соблюдением следующих условий:

- документирование изменений в соответствующем журнале;
- уведомление работника, которого касается изменение;
- анализ претензий, в случае если это изменение причинило кому-нибудь вред;
- разработка планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

12. Для защиты от вредоносных программ и вирусов необходимо использовать только лицензионные или сертифицированные свободно распространяемые антивирусные средства.
13. Для защиты серверов и рабочих станций используются:

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;
- утилиты для обнаружения и анализа новых вирусов.

14. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.
15. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.
16. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. После установки (изменения) программного обеспечения рабочей станции необходимо провести антивирусную проверку.
17. Запуск антивирусных программ осуществляется автоматически по заданию, созданному с использованием планировщика задач, входящего в поставку операционной системы либо поставляемого вместе с антивирусными программами.
18. Антивирусный контроль рабочих станций проводится ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка осуществляется не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется проводить полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.
19. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т. п.). Контроль информации проводится антивирусными средствами в процессе или сразу после

ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.
20. Устанавливаемое на серверы программное обеспечение предварительно проверяется администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.
21. На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

- осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;
- проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

22. На серверах электронной почты необходимо применять антивирусное программное обеспечение, позволяющее осуществлять проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения блокируется. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.
23. Антивирусные базы на всех рабочих станциях и серверах необходимо регулярно обновлять.
24. Администратор системы должен проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которых распространяются вирусы. При обнаружении зараженных вирусом файлов администратору необходимо выполнить следующие действия:

- отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;
- немедленно сообщить о факте обнаружения вирусов непосредственному начальнику, в т. ч. указать предположительный источник (отправитель, владелец и т. д.) зараженного файла, тип зараженного файла, тип вируса, а также рассказать о характере содержащейся в файле информации и выполненных антивирусных мероприятиях.

25. Если администратор системы, обрабатывающей персональные данные, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, он должен определить системные ресурсы, безопасность которых была нарушена, и установить:

- была ли попытка несанкционированного доступа (далее – НСД);
- когда, как и при каких обстоятельствах была предпринята попытка НСД;
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- какова была мотивация нарушителя;
- точку входа нарушителя в систему;
- была ли попытка НСД успешной.

26. Для выявления попытки НСД необходимо:

- установить, какие пользователи в настоящее время работают в системе и на каких рабочих станциях;
- выявить подозрительную активность пользователей, проверить, все ли пользователи вошли в систему со своих рабочих мест и не работает ли кто из них в системе необычно долго;
- убедиться, что никто из пользователей не использует подозрительные программы или программы, не относящиеся к его области деятельности.

27. При анализе системных журналов администратор должен:
проверить наличие подозрительных записей в системных журналах, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны были отсутствовать в этот период времени, а также входы в систему из неожиданных мест, в необычное время и на короткий период времени;

- убедиться в том, что системный журнал не уничтожен и в нем отсутствуют пробелы;
- просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;
- проверить наличие исходящих сообщений электронной почты, адресованных подозрительным хостам;
- проверить журналы на наличие мест, которые выглядят необычно;
- выявить неудачные попытки входа в систему.

28. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) следует проверить:

- нет ли в них подозрительных записей, сделанных в период предполагаемой попытки НСД;
- есть ли в них пробелы, а также места, которые выглядят необычно;
- были ли попытки изменения таблиц маршрутизации и адресных таблиц.

Кроме того, необходимо проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

29. Для обнаружения в системе следов, оставленных злоумышленником в виде файлов, вирусов, троянских программ, изменения системной конфигурации следует:

- составить базовую схему того, как обычно выглядит система;
- провести поиск подозрительных файлов, скрытых файлов, имен файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;
- оценить целостность системных программ;
- проверить систему аутентификации и авторизации.

30. Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.

31. Работники подразделений ДОУ и лица, выполняющие работы по договорам и контрактам, имеющие отношение к проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных, должны быть ознакомлены с Инструкцией под расписку.

Приложение № 7
к приказу № 51 /01-15

Инструкция по организации парольной защиты

1. Общие положения

1.1. Инструкция по организации парольной защиты (далее – Инструкция) призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах дошкольного образовательного учреждения (далее – ДОУ), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах информационной системы (далее – ИС) ДОУ и контроль за действиями исполнителей и обслуживающего персонала при работе с паролями возлагается на системного администратора ДОУ.

2. Правила формирования паролей

2.1. Личные пароли генерируются и распределяются централизованно либо выбираются пользователями информационной системы самостоятельно с учетом следующих требований:

- пароль должен состоять не менее чем из шести символов;
- в пароле обязательно должны присутствовать буквы из верхнего и нижнего регистров, цифры или специальные символы (@, #, $, &, *, % и т. п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. д.), последовательности символов и знаков (111, qwerty, abcd и т. д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т. п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- при смене пароля новый пароль должен отличаться от старого не менее чем в шести позициях.

2.2. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников центра дистанционного образования.

2.3. При технологической необходимости использования имен и паролей некоторых работников (исполнителей) в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.) такие работники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передать на хранение ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для их опечатывания рекомендуется использовать печать отдела кадров.

3. Ввод пароля

При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.).

4. Порядок смены личных паролей

4.1. Смена паролей проводится регулярно, не реже одного раза в три месяца.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) системный администратор должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.

4.3. Срочная (внеплановая) полная смена паролей производится в случае прекращения полномочий (увольнение, переход на другую работу и т. п.) администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 2.1 Инструкции и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

4.5. Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

5. Хранение пароля

5.1. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе либо в сейфе у системного администратора или руководителя подразделения в опечатанном пенале.

5.2. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

5.3. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6. Действия в случае утери и компрометации пароля

В случае утери или компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 4.3 или п. 4.4 Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Ответственность при организации парольной защиты

7.1. Владельцы паролей должны быть ознакомлены под расписку с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.

7.2. Ответственность за организацию парольной защиты в структурных подразделениях ДОУ возлагается на системного администратора.

7.3. Работники ДОУ и лица, имеющие отношение к обработке персональных данных в информационных системах ДОУ, должны быть ознакомлены с Инструкцией под расписку.

Согласовано

Председатель ППО МБДОУ г. Мурманска № 104

_____ Бессолицина С.М.

Приказ № 51/01-15

« _15__» _апреля_ 2016 года

Утверждено

заведующая МБДОУ г. Мурманска № 104

_____ Смирнова Е.С.

Приказ № 51/01-15

« __15__» __апреля_ 2016 года

Положение о защите персональных данных работников в муниципальном бюджетном дошкольном образовательном учреждении г. Мурманска № 104

Мурманск

2016

Положение о защите персональных данных работников в муниципальном бюджетном дошкольном образовательном учреждении г. Мурманска № 104

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о защите персональных данных работников муниципального бюджетного дошкольного образовательного учреждения г. Мурманска № 104, далее по тексту – «Положение» разработано в соответствии с Конституцией РФ, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации, уставом муниципального бюджетного дошкольного образовательного учреждения г. Мурманска № 104 , далее по тексту – «МБДОУ г. Мурманска № 104».

1.2. Под «персональными данными» работника понимается информация, необходимая Организации в связи с трудовыми отношениями и касающаяся конкретного работника, в том числе его:

фамилия, имя, отчество
год, месяц, дата и место рождения
адрес
семейное, социальное, имущественное положение
образование
профессия
доходы
другая информация (данные СНИЛС, ИНН, страхового полиса и др.)

1.3. Под «работником» в Положении понимается лицо, состоящее в трудовых отношениях с МБДОУ.

1.4. Под «должностными лицами» в Положении понимаются работники, состоящие в трудовых отношениях с МБДОУ и имеющие право на получение, обработку, передачу в процессе работы персональных данных (руководящий состав: заведующая и его заместители, руководители структурных подразделений и их заместители; делопроизводитель, работники отдела кадров, бухгалтерии, отдела компьютерных технологий, члены комиссии по социальному страхованию). Обязанность должностных лиц соблюдать Положение должна быть закреплена в трудовых договорах, заключаемых с указанными лицами.

1.5. Под «третьими лицами» в Положении понимаются любые лица (работники, юридические лица, должностные лица государственных органов и органов местного самоуправления, правоохранительных органов), не являющиеся стороной индивидуального трудового договора, заключенного с МБДОУ в лице ее руководителя.

1.6. Положение устанавливает порядок обработки персональных данных работников, их права и обязанности в области защиты персональных данных, порядок передачи персональных данных в Организации и за ее пределы, ответственность должностных лиц за нарушение норм Положения.

1.7. При приеме на работу (до заключения трудового договора) работник должен быть ознакомлен с Положением, заполнить согласие на обработку персональных данных (приложение № 1 к Положению о защите персональных данных работников в муниципальном бюджетном дошкольном образовательном учреждении г. Мурманска № 104).

2. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. К персональной документации (содержащей персональные данные) относятся документы, которые содержат индивидуальные данные о конкретном работнике и используются должностными лицами при исполнении своих должностных обязанностей.

К ним относятся:

1) документы, предъявляемые при трудоустройстве на работу в соответствии с соответствующей статьей Трудового кодекса РФ (65):

паспорт или иной документ, удостоверяющий личность;

трудовая книжка,

страховое свидетельство государственного пенсионного страхования,

документы воинского учета – для военнообязанных и лиц, подлежащих призыву;

документ об образовании, квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки),

направление службы занятости

2) характеристики

3) рекомендательные письма

4) справки, подтверждающие периоды работы у работодателей и размер заработной платы

5) наградные документы

6) справка о наличии/отсутствии судимости

7) медицинские справки

8) организационно-распорядительные документы (приказы, распоряжения), локальные нормативные акты, перечни, списки и иные внутренние документы Организации, содержащие персональные данные работников (фамилию, имя, отчество и др.)

9) документы, подтверждающие предполагаемые и фактически полученные работником денежные средства (приказы по личному составу о приеме на работу, о переводе на работу, о поощрении, расчетные листки)

10) иные документы, содержащие персональные сведения о работниках.

3. ОБЯЗАННОСТИ ДОЛЖНОСТНЫХ ЛИЦ

2.1. При обработке персональных данных работника (получении, хранении, комбинировании, передаче или любом другом использование персональных данных работника), должностные лица, которые имеют к ним доступ и используют при исполнении должностных обязанностей, должны соблюдать следующие требования:

1) обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

2) все персональные данные работника следует получать у него самого.

Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее (не позднее чем за 3 рабочих дня) и от него должно быть получено **письменное согласие**.

Должностные лица должны сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

4) должностные лица не вправе получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни;

5) должностные лица не вправе получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, необходимых для решения вопроса об увольнении

работников по основаниям, предусмотренным пунктами 2, 3 и 5 части первой статьи 81 Трудового кодекса РФ;

6) при принятии решений, затрагивающих интересы работника, должностные лица не вправе основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4. ПРАВА РАБОТНИКОВ

2.1. Работники, предоставившие должностным лицам персональные данные, имеют право на:

свободный **бесплатный** доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

определение своих представителей для защиты своих персональных данных;

доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства.

При отказе должностных лиц исключить или исправить персональные данные работники имеют право подать заявление заведующей МБДОУ о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера (содержащиеся, например, в характеристике, аттестационном листе) работники имеют право дополнить заявлением, выражающим его собственную точку зрения;

требование об извещении МБДОУ всех лиц, которым ранее были сообщены неверные или неполные персональные данные работников, обо всех произведенных в них исключениях, исправлениях или дополнениях;

обжалование в суд любых неправомерных действий или бездействия МБДОУ при обработке и защите их персональных данных.

5. ПОРЯДОК СБОРА И ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Должностные лица имеют право получать только те персональные данные работника, которые необходимы для выполнения конкретных трудовых функций.

4.2. Должностные лица не вправе запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции (например, при решении вопроса о переводе работника на другую должность (работу) при наличии медицинского заключения, дающего основания полагать о невозможности выполнения работником трудовой функции на условиях, предусмотренных трудовым договором, или привлечение работника для определенных видов работ(например: работы на высоте)).

4.3. Должностные лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

4.4. Должностные лица не имеют права сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральными законами (Трудовым кодексом РФ, Налоговым кодексом РФ, Федеральными законами «О статусе судей в Российской Федерации», «О милиции», «О федеральной службе безопасности», «О прокуратуре Российской Федерации», «О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)» и др.), предусматривающими право

должностных лиц контролирующих и правоохранительных органов запрашивать у работодателей в установленном порядке документы, содержащие персональные данные работника - в целях исполнения возложенных на них федеральными законами обязанностей.

5. ПРАВИЛА ХРАНЕНИЯ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.1. Личные дела и трудовые книжки работников хранятся в металлических шкафах, сейфах, имеющих надежные запоры.

5.2. Личные дела предоставляются в распоряжение должностных лиц лишь в следующих случаях:

необходимости оформления наградных документов;

формирования статистических данных;

подготовки характеристики

и при наличии соответствующей резолюции заведующей МБДОУ или его заместителя, заместителя по кадровым вопросам на служебной записке соответствующей формы.

Личные дела выдаются под роспись в журнале выдачи личных дел.

Личное дело должно быть возвращено в МБДОУ в течение недельного срока с момента его получения.

5.3. Трудовые книжки работников могут предоставляться работниками отдела кадров лишь работникам бухгалтерии и членам комиссии по социальному страхованию, - при необходимости проверки данных о страховом стаже работников, - для решения вопросов о правильности исчисления и выплаты пособий по государственному социальному страхованию.

5. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОЛОЖЕНИЯ

Должностные лица, виновные в нарушении Положения, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с Трудовым кодексом РФ, Кодексом Российской Федерации об административных правонарушениях, Уголовным кодексом Российской Федерации.

приложение № 1 к Положению о защите персональных данных воспитанников и родителей (законных представителей воспитанников) в муниципальном бюджетном дошкольном образовательном учреждении г. Мурманска № 104

СОГЛАСИЕ
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____

фамилия, имя, отчество родителя, законного представителя ребенка

документ, удостоверяющий личность _____ серия _____ номер _____

наименование документа

выдан « __ » _____ 20 ____ г. _____

когда и кем выдан

_____

адрес регистрации _____

даю свое согласие на обработку в МБДОУ г. Мурманска № 104 моих персональных данных и данных моего ребенка, относящихся исключительно к перечисленным ниже категориям персональных данных:

-ребенок: ФИО (ребенок), дата рождения, место рождения, пол, СНИЛС, гражданство, реквизиты свидетельства о рождении, адрес регистрации по месту жительства, адрес регистрации по месту пребывания, адрес фактического места жительства, информация о трудной жизненной ситуации, родители (или иные законные представители);

- Мать, отец: ФИО, дата рождения, СНИЛС, гражданство, реквизиты документа, удостоверяющего личность, данные реквизитов банка (для оформления документов на компенсацию части родительской оплаты), данные о доходах, месте работы, состоянии на учете в социальных службах (для оформления льготы по оплате за посещения ребенком МБДОУ)

- законный представитель, не являющийся родителем: тип законного представителя, ФИО, дата рождения, СНИЛС, гражданство, реквизиты документа, удостоверяющего личность, документ, удостоверяющий положение законного представителя по отношению к ребенку.

Я _____

фамилия, имя, отчество

даю согласие на использование персональных данных в целях учета в электронном виде в автоматизированной информационной системе «Электронный детский сад» для реализации полномочий МБДОУ г. Мурманска № 104

Настоящее согласие предоставляется мной на осуществление действий в отношении моих персональных данных и персональных данных моего ребенка, которые необходимы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу третьим лицам для осуществления действий по обмену информацией, обезличивание, блокирование персональных данных, а также осуществление любых иных действий, предусмотренных действующим законодательством РФ.

Я проинформирован, что МБДОУ г. Мурманска № 104 гарантирует обработку моих персональных данных в соответствии с действующим законодательством РФ как неавтоматизированным, так и автоматизированным способами.

Данное согласие действует до достижения целей обработки персональных данных или в течение срока хранения информации.

Данное согласие может быть отозвано в любой момент по моему письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих интересах.

«_____» _____ 201__ г. (_____) _____

подпись *фамилия, имя, отчество*

приложение № 2 к Положению о защите персональных данных воспитанников и родителей (законных представителей воспитанников) в муниципальном бюджетном дошкольном образовательном учреждении г. Мурманска № 104

СОГЛАСИЕ
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ В АИС «ЭЛЕКТРОННЫЙ ДЕТСКИЙ САД»
(в соответствии с требованиями ст.6ФЗ от 27.07.2006 г. №152-ФЗ « О персональных данных»)

Я, _____
(ФИО родителя, законного представителя)

Зарегистрированный по адресу:_____

Основной документ, удостоверяющий личность (серия, номер, кем выдан, дата)_____

Даю согласие муниципальному бюджетному дошкольному образовательному учреждению г. Мурманска №104 (183040, г. Мурманск, ул. Аскольдовцев, д.14), в лице заведующей Смирновой Евгении Сергеевны на обработку и передачу моих персональных данных и данных моего ребенка в АИС «Электронный детский сад» необходимых для выполнения конкретных функций, заданий при полном соблюдении конфиденциальности:

- Фамилия, имя, отчество
- Дата рождения
- Серия, номер, кем выдан, дата выдачи основного документа, удостоверяющего личность
- Адрес регистрации/проживания, телефон, адрес электронной почты
- Образование
- Данные с места работы
- Данные свидетельства о рождении ребенка
- Данные о составе семьи
- Данные о состоянии здоровья
- Национальность
- Данные СНИЛС (ребенка и родителей)

Согласие действительно на период действия основного договора с родителями.
Данное согласие может быть отозвано по моему письменному заявлению.

_____ _____ _____
(дата) (подпись) (ФИО родителя, законного представителя)

приложение № 1 к Положению о защите персональных данных работников в муниципальном бюджетном дошкольном образовательном учреждении г. Мурманска № 104

СОГЛАСИЕ

на обработку персональных данных

(в соответствии с требованиями ст. 6. Федерального закона от 27.07.2006г № 152-ФЗ «О персональных данных»)

Я, _____,
ФИО

зарегистрированный по адресу:_____
_____,

Основной документ, удостоверяющий личность _____
_____
_____

даю согласие Муниципальному бюджетному дошкольному образовательному учреждению г.Мурманска № 104 (183040, г.Мурманск, ул. Аскольдовцев дом 14), в лице заведующей Смирновой Евгении Сергеевны на обработку и передачу моих персональных данных и данных, содержащихся в моем личном деле и трудовой книжке, а также других данных, необходимых для выполнения конкретных функций, заданий при полном соблюдении конфиденциальности:

- фамилия, имя, отчество;
- дата рождения;
- номер основного документа, удостоверяющего личность;
- адрес регистрации/ проживания
- образование;
- данные с места работы;
- данные свидетельства о рождении ребёнка и другие.

Согласие вступает в силу со дня его подписания и действительно на период действия основного договора между МБДОУ г. Мурманск № 104 и мной - работником МБДОУ г. Мурманска № 104.

Согласие может быть отозвано мной в любое время на основании моего письменного заявления.

Я утверждаю, что ознакомлен с Положением об обработке и защите персональных данных работников МБДОУ г.Мурманска № 104, устанавливающим порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

_____ _____ _____

Дата	Подпись	ФИО

Согласовано

Инспектор по охране детства г. Мурманска № 104

_____ _____

Приказ № 51/01-15

« _15__» _апреля_ 2016 года

Утверждено

заведующая МБДОУ г. Мурманска № 104

_____ Смирнова Е.С.

Приказ № 51/01-15

« __15__» __апреля_ 2016 года

Положение о защите персональных данных воспитанников и родителей

(законных представителей воспитанников)

в муниципальном бюджетном дошкольном образовательном

учреждении г. Мурманска № 104

Мурманск

2016

Положение о защите персональных данных воспитанников и родителей (законных представителей воспитанников) в муниципальном бюджетном дошкольном образовательном учреждении г. Мурманска № 104

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о защите персональных данных воспитанников и родителей (законных представителей воспитанников) муниципального бюджетного дошкольного образовательного учреждения г. Мурманска № 104, далее по тексту – «Положение» разработано в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», уставом муниципального бюджетного дошкольного образовательного учреждения г. Мурманска № 104 , далее по тексту – «МБДОУ г. Мурманска № 104».

1.2. Под «персональными данными» воспитанников и родителей (законных представителей воспитанников) понимается информация, необходимая Организации в связи с договорными отношениями и касающаяся конкретного воспитанника и его родителей (законных представителей воспитанников), в том числе:

-ребенок: ФИО (ребенок), дата рождения, место рождения, пол, СНИЛС, гражданство, реквизиты свидетельства о рождении, адрес регистрации по месту жительства, адрес регистрации по месту пребывания, адрес фактического места жительства, информация о трудной жизненной ситуации, информация по состоянию здоровья(при необходимости) родители (или иные законные представители);

- мать, отец: ФИО, дата рождения, СНИЛС, гражданство, реквизиты документа, удостоверяющего личность, данные реквизитов банка (для оформления документов на компенсацию части родительской оплаты), данные о доходах, месте работы, состоянии на учете в социальных службах (для оформления льготы по оплате за посещения ребенком МБДОУ);

- законный представитель, не являющийся родителем: тип законного представителя, ФИО, дата рождения, СНИЛС, гражданство, реквизиты документа, удостоверяющего личность, документ, удостоверяющий положение законного представителя по отношению к ребенку.

В связи с тем, что персональные данные родителей и детей используются при работе в АИС « электронный детский сад» под «персональными данными» воспитанников и родителей (законных представителей воспитанников) для размещения в АИС понимается информация, необходимая Организации в связи с договорными отношениями и касающаяся конкретного воспитанника и его родителей (законных представителей воспитанников), в том числе:

- Фамилия, имя, отчество
- Дата рождения
- Серия, номер, кем выдан, дата выдачи основного документа, удостоверяющего личность
- Адрес регистрации/проживания, телефон, адрес электронной почты
- Образование
- Данные с места работы
- Данные свидетельства о рождении ребенка
- Данные о составе семьи
- Данные о состоянии здоровья

- Национальность
- Данные СНИЛС (ребенка и родителей)

1.3. Под «родителем» в Положении понимается лицо, состоящее в договорных отношениях с МБДОУ, являющееся родителем или законным представителем ребенка (воспитанника).

1.4. Под «должностными лицами» в Положении понимаются работники, состоящие в договорных отношениях с «родителями» и имеющие право на получение, обработку, передачу в процессе работы персональных данных (руководящий состав: заведующая и его заместители, руководители структурных подразделений и их заместители; делопроизводитель, работники отдела кадров, бухгалтерии, отдела компьютерных технологий, члены комиссии по защите прав детства). Обязанность должностных лиц соблюдать Положение должна быть закреплена в виде подписи под данным положением.

1.5. Под «третьими лицами» в Положении понимаются любые лица (работники, юридические лица, должностные лица государственных органов и органов местного самоуправления, правоохранительных органов), не являющиеся стороной договора, заключенного с МБДОУ в лице ее руководителя.

1.6. Положение устанавливает порядок обработки персональных данных воспитанников и родителей (законных представителей воспитанников), их права и обязанности в области защиты персональных данных, порядок передачи персональных данных в Организации и за ее пределы, ответственность должностных лиц за нарушение норм Положения.

1.7. При приеме ребенка в МБДОУ (до заключения договора) «родитель» должен быть ознакомлен с Положением, заполнить согласия на обработку персональных данных (приложение № 1, № 2 к Положению о защите персональных данных воспитанников и родителей (законных представителей воспитанников) в муниципальном бюджетном дошкольном образовательном учреждении г. Мурманска № 104).

2. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. К персональной документации (содержащей персональные данные) относятся документы, которые содержат индивидуальные данные о конкретном ребенке, его «родителях» и используются должностными лицами при исполнении своих должностных обязанностей.

К ним относятся:

-ребенок: ФИО (ребенок), дата рождения, место рождения, пол, СНИЛС, гражданство, реквизиты свидетельства о рождении, адрес регистрации по месту жительства, адрес регистрации по месту пребывания, адрес фактического места жительства, информация о трудной жизненной ситуации, информация по состоянию здоровья (при необходимости) родители (или иные законные представители);

- мать, отец: ФИО, дата рождения, СНИЛС, гражданство, реквизиты документа, удостоверяющего личность, данные реквизитов банка (для оформления документов на компенсацию части родительской оплаты), данные о доходах, месте работы, состоянии на учете в социальных службах (для оформления льготы по оплате за посещения ребенком МБДОУ);

- законный представитель, не являющийся родителем: тип законного представителя, ФИО, дата рождения, СНИЛС, гражданство, реквизиты документа, удостоверяющего личность, документ, удостоверяющий положение законного представителя по отношению к ребенку.

при работе в АИС « электронный детский сад» :

- Фамилия, имя, отчество
- Дата рождения
- Серия, номер, кем выдан, дата выдачи основного документа, удостоверяющего личность
- Адрес регистрации/проживания, телефон, адрес электронной почты
- Образование

- Данные с места работы
- Данные свидетельства о рождении ребенка
- Данные о составе семьи
- Данные о состоянии здоровья
- Национальность
- Данные СНИЛС (ребенка и родителей)
- Иные документы, содержащие персональные сведения о ребенке, его «родителях».

3. ОБЯЗАННОСТИ ДОЛЖНОСТНЫХ ЛИЦ

2.1. При обработке персональных данных ребенка, « родителей» (получении, хранении, комбинировании, передаче или любом другом использование персональных данных), должностные лица, которые имеют к ним доступ и используют при исполнении должностных обязанностей, должны соблюдать следующие требования:

1) обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, обеспечения личной безопасности;

2) все персональные данные ребенка и его « родителей» следует получать у родителей (законных представителей) ребенка, исключая третьих лиц.

Если персональные данные ребенка, « родителя» возможно получить только у третьей стороны, то «родитель» должен быть уведомлен об этом заранее (не позднее чем за 3 рабочих дня) и от него должно быть получено **письменное согласие**.

Должностные лица должны сообщить «родителю» о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа «родителя» дать письменное согласие на их получение;

4) должностные лица не вправе получать и обрабатывать персональные данные «родителя» и воспитанника о его политических, религиозных и иных убеждениях и частной жизни;

5) должностные лица не вправе получать и обрабатывать персональные данные «родителя» и воспитанника о его членстве в общественных объединениях;

4. ПРАВА воспитанников, родителей (законных представителей воспитанников)

2.1. «Родители», предоставившие должностным лицам персональные данные, имеют право на:

свободный **бесплатный** доступ к своим персональным данным, данным своего ребенка, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законом;

определение своих представителей для защиты своих персональных данных;

доступ к относящимся к ним медицинским данным (данным ребенка) с помощью медицинского специалиста по их выбору;

требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства.

При отказе должностных лиц исключить или исправить персональные данные «родители» имеют право подать заявление заведующей МБДОУ о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера (содержащиеся, например, в характеристике) «родители» имеют право дополнить заявлением, выражающим его собственную точку зрения;

требование об извещении МБДОУ всех лиц, которым ранее были сообщены неверные или неполные персональные данные «родителей», обо всех произведенных в них исключениях, исправлениях или дополнениях;

обжалование в суд любых неправомерных действий или бездействия МБДОУ при обработке и защите их персональных данных.

5. ПОРЯДОК СБОРА И ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Должностные лица имеют право получать только те персональные данные родителей (законных представителей воспитанников),воспитанников, которые необходимы для выполнения конкретных функций ОУ.

4.2. Должностные лица не вправе запрашивать информацию о состоянии здоровья « родителя», воспитанника, за исключением тех сведений, которые относятся к вопросу о возможности:

- распределения в группы (например, при решении вопроса о переводе в группу компенсирующей направленности или в коррекционную группу, при наличии медицинского заключения, дающего основания полагать о необходимости предоставления дополнительных воспитательно - образовательных услуг)

- определения мер для инклюзивного образования, проведения мероприятий по выполнению программы реабилитации (дети - инвалиды)).

4.3. Должностные лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами.

4.4. Должностные лица не имеют права сообщать персональные данные третьей стороне без письменного согласия «родителя», за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью воспитанников, а также в случаях, установленных федеральными законами (Федеральными законами «О статусе судей в Российской Федерации», «О милиции», «О федеральной службе безопасности», «О прокуратуре Российской Федерации», «О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)» и др.), предусматривающими право должностных лиц контролирующих и правоохранительных органов запрашивать у администрации ДОУ в установленном порядке документы, содержащие персональные данные «родителя», воспитанников - в целях исполнения возложенных на них федеральными законами обязанностей.

5. ПРАВИЛА ХРАНЕНИЯ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.1. Личные дела воспитанников хранятся в шкафах, сейфах, не имеющих доступ посторонних лиц.

5.2. Личные дела предоставляются в распоряжение должностных лиц лишь в следующих случаях:

необходимости оформления документов;

формирования статистических данных;

подготовки характеристики

и при наличии соответствующей резолюции заведующей МБДОУ или его заместителя, заместителя по кадровым вопросам на служебной записке соответствующей формы.

Личные дела выдаются под роспись в журнале выдачи личных дел.

Личное дело должно быть возвращено в МБДОУ в течение недельного срока с момента его получения.

5. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОЛОЖЕНИЯ

Должностные лица, виновные в нарушении Положения, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии

с Трудовым кодексом РФ, Кодексом Российской Федерации об административных правонарушениях, Уголовным кодексом Российской Федерации.

Приложение № 1 к приказу
№ 64/01-15 от 28.04.2017 г.

Обязательство

о неразглашении персональных данных работников, членов семей работников, воспитанников, членов семей воспитанников, а также других данных, ставших известными при выполнении необходимых мероприятий для выполнения конкретных функций, заданий при полном соблюдении конфиденциальности

(в соответствии с требованиями Федерального закона от 27.07.2006г № 152-ФЗ «О персональных данных»).

Я, _____,
ФИО

зарегистрированный по адресу:_____
_____,

Основной документ, удостоверяющий личность _____
_____
_____

Обязуюсь не разглашать персональные данные работников, членов семей работников, воспитанников, членов семей воспитанников, а также других данных, ставших известными мне в связи с исполнением своих должностных обязанностей в муниципальном бюджетном дошкольном образовательном учреждении г.Мурманска № 104 (183040, г.Мурманск, ул. Аскольдовцев, дом 14).

Об ответственности за разглашение персональных данных предупреждена, с требованиями Федерального закона от 27.07.2006г № 152-ФЗ «О персональных данных» ознакомлена.

Обязательство вступает в силу со дня его подписания.

Я утверждаю, что ознакомлена с Положением об обработке и защите персональных данных работников МБДОУ г.Мурманска № 104,воспитанников и родителей (законных представителей МБДОУ г. Мурманска № 104) устанавливающим порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

_____	_____	_____
Дата	Подпись	ФИО

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
г. МУРМАНСКА № 104

Номер документа	Дата составления
105 /01-15	05.09.2017 г.

ПРИКАЗ

«О внесении дополнений в приказ № 51/01-15
от 15.04.2017 года « О порядке обработки
и защите персональных данных
в МБДОУ г. Мурманска № 104»

Согласно Федеральному закону от 23.12.2010 № 359-ФЗ «О внесении изменения в статью 25 Федерального закона "О персональных данных", образовательное учреждение (далее – ОУ) должно привести информационные системы персональных данных в соответствие с требованиями Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее – Закон № 152-ФЗ) в соответствии с вышеизложенным приказываю:

1. Внести дополнения в пункт 3 приказа № 51/01-15 от 15.04.2017 года « О порядке обработки и защите персональных данных в МБДОУ г. Мурманска № 104» :

Возложить персональную ответственность за организацию защиты персональных данных работников, членов семей работников, воспитанников, членов семей воспитанников, а также других данных, ставших известными при выполнении необходимых мероприятий для выполнения конкретных функций, заданий при полном соблюдении конфиденциальности с 05.09.2017 года на педагогических сотрудников, которые при выполнении должностных обязанностей имеют доступ к персональным данным: при оформлении тетради сведений о родителях, получении доверенностей на ребенка и членов семьи воспитанников, при оформлении тетради здоровья, оформлении «зрительных уголков», получении информации о диагнозах воспитанников, нарушениях в здоровье, в освоении программ воспитанниками, ставшую известной в ходе осуществления педагогических мероприятий (педагогических советов, семинаров - практикумов, консультаций, бесед и др.) для соблюдения Кодекса этики МБДОУ г. Мурманска № 104 и нераспространения внутренней информации МБДОУ(приложение № 1 к данному приказу).

2. До 01.10.2017 года (по мере выхода сотрудников с ежегодных отпусков) собрать с сотрудников обязательство о неразглашении персональных данных работников, членов семей работников, воспитанников, членов семей воспитанников, а также других данных, ставших известными при выполнении трудовой функции в МБДОУ г. Мурманска № 104, при выполнении должностных обязанностей, при полном соблюдении конфиденциальности, ознакомить сотрудников с Положением об обработке и защите персональных данных работников МБДОУ г.Мурманска № 104,воспитанников и родителей (законных представителей МБДОУ г. Мурманска № 104) устанавливающим порядок обработки персональных данных, а также с правами и обязанностями сотрудников в этой области.

3. Контроль за выполнением данного приказа оставляю за собой.
Заведующий МБДОУ г. Мурманска № 104 ____ Смирнова Е.С.

Приложение № 1 к приказу
№ 105/01-15 от 05.09.2017 г.

Обязательство

о неразглашении персональных данных работников, членов семей работников, воспитанников, членов семей воспитанников, а также других данных, ставших известными при выполнении трудовой функции в МБДОУ г. Мурманска № 104, при выполнении должностных обязанностей при полном соблюдении конфиденциальности
(в соответствии с требованиями Федерального закона от 27.07.2006г № 152-ФЗ «О персональных данных»).

Я, _____,
ФИО

зарегистрированный по адресу:_____
_____,

Основной документ, удостоверяющий личность _____
_____
_____

Обязуюсь не разглашать персональные данные работников, членов семей работников, воспитанников, членов семей воспитанников, а также других данных, ставших известными мне при выполнении трудовой функции в связи с исполнением своих должностных обязанностей (должностных обязанностей) в муниципальном бюджетном дошкольном образовательном учреждении г.Мурманска № 104 (183040, г.Мурманск, ул. Аскольдовцев, дом 14).

Обязуюсь не разглашать родителям воспитанников информацию, ставшую мне известной в ходе осуществления педагогических мероприятий (педагогических советов, семинаров - практикумов, консультаций, бесед и др.) для соблюдения Кодекса этики МБДОУ г. Мурманска № 104 и нераспространения внутренней информации МБДОУ, в части, касаемо защиты персональных данных воспитанников (диагнозы, освоение программы и другое)

Об ответственности за разглашение персональных данных предупреждена, с требованиями Федерального закона от 27.07.2006г № 152-ФЗ «О персональных данных» ознакомлена.

Обязательство вступает в силу со дня его подписания.

Я утверждаю, что ознакомлена с Положением об обработке и защите персональных данных работников МБДОУ г.Мурманска № 104,воспитанников и родителей (законных представителей МБДОУ г. Мурманска № 104) устанавливающим порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

_____ _____ _____

Дата Подпись ФИО

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
г. МУРМАНСКА № 104

Номер документа	Дата составления
11/01-15	14.01.2018 г.

О внесении изменений и дополнений
в приказ № 51/01-15 от 15.04.2016 года
«О порядке обработки и защите
персональных данных в
МБДОУ г. Мурманска № 104»

Согласно Федеральному закону от 23.12.2010 № 359-ФЗ «О внесении изменения в статью 25 Федерального закона "О персональных данных", образовательное учреждение (далее – ОУ) должно привести информационные системы персональных данных в соответствие с требованиями Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее – Закон № 152-ФЗ) в соответствии с вышеизложенным, в связи со сменой секретаря(с функционалом контрактного управляющего), старшего воспитателя) приказываю:

1. Ознакомить Иванову А.А., старшего воспитателя и Смирнову А.В. секретаря с функционалом контрактного управляющего) с Положением о защите персональных данных работников в муниципальном бюджетном дошкольном образовательном учреждении г. Мурманска № 104 (в которое включен порядок обработки и защиты персональных данных) с приложением № 1 – формой согласия на обработку персональных данных;

2. Ознакомить Иванову А.А., старшего воспитателя и Смирнову А.В. секретаря с функционалом контрактного управляющего) Положением о защите персональных данных воспитанников и родителей (законных представителей воспитанников) в муниципальном бюджетном дошкольном образовательном учреждении г. Мурманска № 104 (в которое включен порядок обработки и защиты персональных данных) с приложением № 1 – формой согласия на обработку персональных данных, приложением № 2 – формой согласия на обработку персональных данных в АИС «электронный детский сад»;

3. Возложить персональную ответственность за организацию защиты персональных данных сотрудников, воспитанников МБДОУ, родителей (законных представителей МБДОУ) с 01.02.2018 года на сотрудников, которые при выполнении должностных обязанностей имеют доступ к персональным данным: Иванову А.А., старшего воспитателя и Смирнову А.В. секретаря с функционалом контрактного управляющего).

4. Назначить лицом, ответственным за техническое администрирование организации защиты персональных данных – делопроизводителя Смирнову В.С. с 01.02.2018 года. В ее отсутствие ответственность возлагается на сотрудника, замещающего данную должность по приказу (с ознакомлением с данным приказом и всеми документами по данному приказу), при отсутствии замены - на заведующую МБДОУ – Смирнову Е.С.

6. Ознакомить Иванову А.А., старшего воспитателя и Смирнову А.В. секретаря с функционалом контрактного управляющего) с организационно-нормативными документами ,содержащимися в приказе № 51/01-15 от 15.04.2016 года «О порядке обработки и защите персональных данных в МБДОУ г. Мурманска № 104»

- список работников ДОУ, допущенных к обработке персональных данных (приложение 1 к приказу);
- форма журнала обращений по ознакомлению с персональными данными (приложение 2 к приказу);
- различные формы анкет для воспитанников и их родителей (законных представителей) (приложение 3 к приказу);
- инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (приложение 4 к приказу);
- инструкция пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники (приложение 5 к приказу);
- инструкция по проведению мониторинга информационной безопасности и антивирусного контроля (приложение 6 к приказу);
- инструкция по организации парольной защиты (приложение 7 к приказу).

7. Сотрудникам, ответственным за обработку и защиту персональных данных руководствоваться в своей деятельности нормативными документами:

- Федеральный закон от 23.12.2010 № 359-ФЗ «О внесении изменения в статью 25 Федерального закона "О персональных данных"»
- Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" (ред. от 23.12.2010)
- Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (ред. от 06.04.2011)
- Федеральный закон от 02.05.2006 № 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации" (ред. от 27.07.2010)

8. Делопроизводителю Смирновой В.С. вести журналы в соответствии с приложением № 1,2.

9. Контроль за выполнением данного приказа оставляю за собой.

Заведующая МБДОУ г. Мурманска № 104 ____ Смирнова Е.С.