МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД № 48 «ОДУВАНЧИК» Г.СВЕТЛОГРАД.

ВЫПИСКА ИЗ ПРИКАЗА

от 03.09.2018г. № 117/1

«Об утверждении документов
и перечня персональных данных,
обрабатываемых в МБДОУ ДС
№48 «Одуванчик» г. Светлоград

На основании пункта 1 Перечня сведений конфиденциального характера, утвержденного Указом Президента РФ от 27 июля 2006г. №152 «О персональных данных», а также в соответствии с пунктом 1 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами», утвержденным постановлением Правительства РФ от 21 марта 2012 г.№ 211

ПРИКАЗЫВАЮ:

1.Утвердить перечень персональных данных, обрабатываемых в информационной системе персональных данных МБДОУ ДС №48 «Одуванчик» г. Светлоград согласно Приложению №1.

2. Утвердить перечень должностей работников МБДОУ, замещение которых предусматривает обработку персональных данных, либо доступа к персональным данным. Приложение №2

3. Утвердить должностную инструкцию ответственного за обработку персональных данных в учреждении. Приложение №3

4.Утвердить Порядок доступа в помещение, в которых ведется обработка персональных данных работников МБДОУ. Приложение №4

5. Утвердить соглашение о неразглашении персональных данных Приложение № 6

6. Контроль над исполнением настоящего приказа оставляю за собой.

Заведующий МБДОУ ДС № 48 «Одуванчик» г. Светлоград Г.Ф.Воронко

Приложение №1
к Приказу №117/1 от 03.09.2018г.

Перечень

персональных данных обрабатываемых в информационной системе персональных данных детей, родителей (законных представителей) воспитанников, работников учреждения в«АВЕРС: Контингент ДОО» Категории персональных данных сотрудников ДОУ, воспитанников и родителей (законных представителей) несовершеннолетних:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- документ удостоверяющий личность;
- адрес регистрации; фактический адрес места жительства;
- фотографии;
- номер полиса обязательного медицинского страхования;
- сведения о состоянии здоровья, находящиеся в медицинской карте
- воспитанника;
- социальное положение;
- жилищные условия;
- документы при установлении опеки; контактные телефоны;
- сведения о гражданстве;
- паспортные данные;
- сведения об образовании;
- воинской обязанности;
- трудовом стаже;
- о предыдущем месте работы;
- составе семьи;
- социальных льготах;
- информация об образовании;
- страховом пенсионом свидетельстве;
- ИНН;
- сведения об аттестации;
- повышении квалификации;
- профессиональной переподготовке;
- сведения о наградах (поощрениях, почетных званиях).

Приложение №2
к Приказу №117/1 от 03.09.2018г.

Перечень
должностей работников МБДОУ ДС №48 «Одуванчик» г. Светлоград, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

1.	Заведующий
2.	Заместитель заведующего по воспитательно-методической работе
3.	Делопроизводитель
4.	Воспитатели всех возрастных групп

Приложение №3
к Приказу №117/1 от 03.09.2018г.

Должностная инструкция ответственного за организацию обработки персональных данных

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Должностная инструкция муниципального бюджетного дошкольного образовательного учреждения детского сада №48 «Одуванчик» г. Светлоград (далее ДОУ) разработана в соответствии с Федеральным законом от 27.07.2006 N 152 - ФЗ «О Персональных данных».

1.2. Цель разработки Инструкции - обеспечение защиты прав работников, воспитанников и родителей (законных представителей) воспитанников ДОУ при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным граждан, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Ответственный за организацию обработки персональных данных является штатным сотрудником ДОУ и назначается приказом заведующего.

1.4. Решение вопросов организации защиты персональных данных в ДОУ входит в прямые служебные обязанности ответственного за организацию обработки персональных данных.

1.5. Порядок ввода в действие и изменения Инструкции.

1.5.1. Настоящая Инструкция вступает в силу с момента ее утверждения заведующего ДОУ.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.2. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.3. Доступ к информации – возможность получения информации и её использования (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.4. Защита информации — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.5. Информация - сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации,

информационных технологиях и защите информации»).
2.6. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. N 152- ФЗ «О персональных данных»).
2.7. Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.
2.8. Носитель информации - любой материальный объект или среда, используемый для хранения или передачи информации.
2.9. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).
2.10. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).
2.11. Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.
2.12. Угрозы безопасности персональных данных (УБПДн) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных (ст. 19 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).
2.13. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

III. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Ответственный за организацию обработки персональных данных обязан:

3.1. Знать перечень и условия обработки персональных данных в ДОУ.

3.2. Знать и предоставлять на утверждение заведующему изменения к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей.

3.3. Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей.

3.4. Осуществлять учёт документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения.

3.5. Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

3.6. Реагировать на попытки несанкционированного доступа к информации в установленном ст.4 настоящей Инструкции порядке.

3.7.Контролировать осуществление мероприятий по установке и настройке средств защиты информации.

3.8.Контролировать оперативное внесение изменений в конфигурацию технических средств ИСПДн, требовать отражения соответствующих изменений в «Техническом паспорте информационной системы персональных данных».

3.9. По указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПДн и правилам обработки персональных данных.

3.10. Проводить занятия и инструктажи с сотрудниками и руководителями структурных подразделений и филиалов о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности персональных данных.

3.11. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

3.12. Контролировать соблюдение сотрудниками локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными.

3.13. Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.

3.14. Организовать учет обращений субъектов персональных данных, контролировать заполнение «Журнала учета обращений субъектов персональных данных» (Приложение 1).
3.15. Представлять интересы ДОУ при проверках надзорных органов в сфере обработки персональных данных.
3.16. Знать законодательство РФ о персональных данных, следить за его изменениями.
3.17. Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

IV. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

4.1. К попыткам несанкционированного доступа относятся:
4.1.1. Сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;
4.1.2. Действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.
4.2. При выявлении факта несанкционированного доступа ответственный за организацию обработки персональных данных обязан:
4.2.1. Прекратить несанкционированный доступ к персональным данным;
4.2.2.Доложить заведующему ДОУ служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;
4.2.3. Известить руководителя структурного подразделения или филиала, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;
4.2.4. Известить администратора безопасности ИСПДн о факте несанкционированного доступа.

V. ПРАВА

Ответственный за организацию обработки персональных данных имеет право:
5.1. Требовать от сотрудников выполнения локальных нормативно-правовых актов в части работы с персональными данными.
5.2. Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.
5.3. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных,

нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

Ответственность:

5.4. Ответственный за организацию обработки персональных данных несёт персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

5.5. Ответственный за организацию обработки персональных данных при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение №4
к Приказу №117/1 от 03.09.2018г.

Порядок доступа в помещение
в котором ведется обработка персональных данных

1. Общие положения.

1. Настоящий порядок доступа (далее – Порядок) работников муниципального бюджетного дошкольного образовательного учреждения детского сада №48 «Одуванчик» г. Светлоград (далее – Учреждение) в помещения контролируемой зоны, в которых ведется обработка персональных данных (далее - ОПД) в информационных системах персональных данных (далее – ИСПДН), устанавливает единые требования к доступу работников Учреждения в помещения, в которых ведется обработка ОПД, которые необходимы для оказания государственных и муниципальных услуг, обеспечения кадровой и бухгалтерской деятельности Учреждения, а также в целях обеспечения соблюдения требований законодательства РФ в области ОПД.

1.2. Настоящий Порядок разработан в соответствии с частью 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденных постановлением Правительства РФ от 21 марта 2012 года №211, и на основании «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденных приказом ФСТЭК России от 11 февраля 2013 года №17, и «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при обработке в информационных системах персональных данных», утвержденных ФСБ России 21 февраля 2008 года №149/6/6-622.

1.3 Контролируемая зона (далее – контролируемая зона), в которой расположены средства автоматизации и защиты ИСПДН, в том числе автоматизированные рабочие места (далее –АРМ), на которых ведется обработка ОПД.

1.4 В перечень помещений, в которых ведется обработка ОПД входят:

- кабинет заведующего Учреждения;
- кабинет секретаря Учреждения.

1.5 Настоящий порядок обязателен для применения и исполнения всеми сотрудниками Учреждения.

1.6 Ответственность за соблюдение положений настоящего Порядка несут работники Учреждения, обрабатывающие ОПД.

1.7 Контроль соблюдения требований настоящего Порядка обеспечивают

ответственные за организацию обработки ОПД в Учреждении.
2. Требования к помещениям контролируемой зоны.
2.1 Бесконтрольный доступ сторонних лиц в помещения контролируемой зоны должен быть исключен.
3. Доступ в помещения контролируемой зоны.
3.1 Доступ посторонних лиц в помещения контролируемой зоны, в отсутствии ответственного за организацию обработки ОПД в Учреждении, должен осуществляться только ввиду служебной необходимости.
3.2. На момент присутствия посторонних лиц в помещении контролируемой зоны, должны быть приняты меры по недопущению ознакомления посторонних лиц с ОПД (например: мониторы повернуты в сторону посетителей, документы убраны в стол, либо находятся в непрозрачной папке или накрыты чистыми листами бумаги).
3.3. В нерабочее время помещения контролируемой зоны должны быть закрыты.
4. Доступ в серверные помещения контролируемой зоны.
4.1 Доступ в помещения контролируемой зоны разрешен ответственным за обеспечение безопасности персональных данных информационных систем персональных данных.
4.2. Учреждения и ответственным за организацию обработки ОПД в Учреждении. Нахождение в помещениях контролируемой зоны посторонних лиц без сопровождающего не допустимо.
5. Требования к помещениям контролируемой зоны.
5.1 Помещения контролируемой зоны должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, необходимо оборудовать металлическими решетками, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.
5.2 Для предотвращения просмотра извне помещений контролируемой зоны их окна должны быть защищены.
5.3 При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за организацию обработки ОПД в Учреждении. Прибывший ответственный за организацию обработки ОПД в Учреждении должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.
5.4 В помещениях, где хранится и обрабатывается информация ОПД, должна быть сведена к минимуму возможность неконтролируемого доступа посторонних лиц к ИСПДн.
5.5 На время отсутствия пользователей криптосредств указанное оборудование, при наличии технической возможности, должно быть выключено. В противном случае по согласованию с ответственным за организацию обработки ОПД В Учреждении необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.