

Приложение 1
к приказу МБОУ «Шарапская СОШ»
от **09.01.2018** № **3** «Об утверждении
организационно-распорядительных
документов по защите персональных
данных»

ПОЛОЖЕНИЕ **об обработке персональных данных** **с использованием средств автоматизации**

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных с использованием средств автоматизации МБОУ «Шарапская СОШ» (далее – Положение) (далее – Учреждение) разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. № 1119 и другими нормативно-правовыми актами, действующими на территории Российской Федерации.

1.2. Цели разработки Положения:

1.2.1. определение порядка обработки персональных данных сотрудников и граждан учреждения, а также иных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий Учреждения;

1.2.2. обеспечение защиты прав и свобод человека и гражданина, в т.ч. сотрудников и граждан учреждения, при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

1.2.3. установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. К любой информации, содержащей персональные данные субъекта, применяется режим конфиденциальности, за исключением:

1.3.1. обезличенных персональных данных;

1.3.2. общедоступных персональных данных.

1.4. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения если иное не определено законом Российской Федерации.

2. Термины и определения

2.1. **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. № 152-ФЗ «О персональных данных»).

2.2. **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. № 152-ФЗ «О персональных данных»).

2.3. **Документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель (ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.4. **Информация** – сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.5. **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.6. **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. № 152-ФЗ «О персональных данных»).

2.7. **Оператор персональных данных** – Учреждение.

2.8. **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. № 152-ФЗ «О персональных данных»).

2.9. **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.10. **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. № 152-ФЗ «О персональных данных»).

3. Состав персональных данных

3.1 Состав персональных данных, обрабатываемых в Учреждение, определяется Перечнем сведений, содержащих персональные данные (Приложение 1).

4. Порядок получения персональных данных

4.1. Персональные данные следует получать непосредственно у субъекта, либо у законного представителя.

4.2. Перед началом обработки персональных данных необходимо получить у субъекта или его законного представителя согласие на обработку персональных данных в письменной форме (приложение 1).

4.3. Комплекс документов, сопровождающий процесс взаимодействия с соискателями вакантной должности:

4.3.1. При наличии вакансии, поиск кандидатов на вакантную должность осуществляется через центр занятости населения, так же выкладывается информация о вакансии на сайт трудоустройства. По результатам собеседования кандидата с руководителем и (или) заместителями руководителя принимается решение о трудоустройстве кандидата на вакантную должность.

4.3.2. В случае если специалист по кадрам учреждения получил резюме в электронном виде, но в данный момент не существует вакантной должности для данного соискателя, специалист по кадрам уничтожает резюме в течение 5 (Пяти) дней.

4.4. Комплекс документов, сопровождающий процесс оформления трудовых отношений сотрудника учреждения при его приёме, переводе и увольнении:

4.4.1. Информация, представляемая сотрудником при поступлении на работу в учреждение, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство обязательного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;

– документ об образовании и (или) о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;

– справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям, выданную в порядке и по форме, которые устанавливаются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, - при поступлении на работу, связанную с деятельностью, к осуществлению которой в соответствии с Трудовым кодексом, иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию;

– справку о том, является или не является лицо подвергнутым административному наказанию за потребление наркотических средств или психотропных веществ без назначения врача либо новых потенциально опасных психоактивных веществ, которая выдана в порядке и по форме, которые устанавливаются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, - при поступлении на работу, связанную с деятельностью, к осуществлению которой в соответствии с федеральными законами не допускаются лица, подвергнутые административному наказанию за потребление наркотических средств или психотропных веществ без назначения врача либо новых потенциально опасных психоактивных веществ, до окончания срока, в течение которого лицо считается подвергнутым административному наказанию.

4.3.2. При оформлении сотрудника в учреждение специалистом по кадрам заполняется унифицированная форма Т-2 – Личная карточка сотрудника.

4.3.3. Вся необходимая информация копируется в ИСПДн.

4.3.4. У специалиста учреждения по кадрам создаются и хранятся следующие группы документов, содержащие персональные данные сотрудников в единичном или сводном виде:

– документы, содержащие персональные данные сотрудников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки сотрудников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации сотрудников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству учреждения, руководителям структурных

подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);

– документация по Учреждению, работе отделов (положения, должностные инструкции сотрудников, приказы руководителя Учреждения);

– документы по планированию, учету, анализу и отчетности в части работы с персоналом учреждения.

5. Порядок хранения персональных данных

5.1. Хранение электронных носителей (дискет, дисков и т.п.), содержащих персональные данные, должно осуществляться в специальных папках, закрытых шкафах или сейфах, в порядке, исключающем доступ к ним третьих лиц.

5.2. Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

5.3. Обработка персональных данных в учреждении осуществляется до утраты правовых оснований обработки персональных данных. Перечень нормативно-правовых актов, определяющих основания обработки персональных данных в учреждении определяются Перечнем сведений, содержащих персональные данные (приложение 2).

5.4. По истечении срока хранения (30 дней, если иное не прописано в нормативно-правовых актах) документы, либо иные материальные носители персональных данных должны быть уничтожены без возможности восстановления с составлением акта. Для машинных носителей допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ без уничтожения материального носителя.

5.5. Обезличивания персональных данных в учреждении не предполагается.

6. Порядок использования персональных данных

8.1. Обработка персональных данных может осуществляться исключительно в целях обработки персональных данных, осуществления трудовых (договорных) отношений, и в случаях, установленных законодательством Российской Федерации.

8.2. При определении объема и содержания, обрабатываемых персональных данных, Учреждение руководствуется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации,

Федеральным законом «О персональных данных», Федеральным законом от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» и иными нормативно-правовыми актами Российской Федерации, а также настоящим Положением.

7. Порядок передачи персональных данных

7.1. Передавать персональные данные субъектов допускается только тем сотрудникам, которые имеют допуск к обработке персональных данных.

7.2. Предоставление персональных данных допускается в случаях передачи Федеральной налоговой службе, Пенсионному фонду России, ПАО «Сбербанк» с целью начисления заработной платы, Фонду обязательного медицинского страхования и т.п., раскрытия данных правоохранительным органам при наличии законных оснований, а также в иных случаях, установленных законодательством РФ.

7.3. Не допускается распространение персональных данных субъекта.

8. Организация защиты персональных данных

8.1. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Учреждением за счет собственных средств.

8.2. Защита персональных данных должна вестись по трём взаимодополняющим направлениям:

8.2.1. Проведение организационных мероприятий:

– разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;

– ознакомление сотрудников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;

– организация учёта носителей персональных данных;

– разработка модели угроз безопасности персональным данным;

– проведение обучения сотрудников вопросам защиты персональных данных.

8.2.2. Программно-аппаратная защита:

– внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом №184 от 27.12.2002 г. «О техническом регулировании» оценку соответствия.

8.2.3. Инженерно-техническая защита:

– установка сейфов или запирающихся шкафов для хранения носителей персональных данных;

– установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.

8.3. Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за организацию обработки персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами Учреждения.

8.4. Организацию и контроль защиты персональных данных в структурных подразделениях Учреждения осуществляют их непосредственные руководители.

9. Порядок предоставления доступа к персональным данным

9.1. Допуск к персональным данным субъекта могут иметь только те сотрудники Учреждения, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей. Перечень таких сотрудников отражен в приказе «Об утверждении списка должностных лиц, которым необходим доступ к персональным данным, обрабатываемым в информационных системах».

9.2. Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:

9.2.1. ознакомление сотрудника с настоящим Положением, инструкцией о порядке работы с персональными данными и другими локальными нормативно-правовыми актами Учреждения, касающимися обработки персональных данных;

9.2.2. истребование с сотрудника обязательства о неразглашении конфиденциальной информации (приложения 4,5).

9.3. Каждый сотрудник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.

9.4. Сотрудникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.

9.5. Специалисты учреждения, которым доступ к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей (далее – пользователи), для получения доступа к информационной системе направляют письменный запрос на имя ответственного за организацию обработки персональных данных.

10. Требования по обеспечению безопасности

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

10.1.1. проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

10.1.2. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

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

10.1.4. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

10.1.5. постоянный контроль над обеспечением уровня защищенности персональных данных.

10.2. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

10.2.1. определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

10.2.2. разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

10.2.3. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

10.2.4. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

10.2.5. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

10.2.6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

10.2.7. учет лиц, допущенных к работе с персональными данными в информационной системе;

10.2.8. контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

10.2.9. разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

10.2.10. описание системы защиты персональных данных.

10.3. Осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе уполномоченным лицом возлагается на администратора безопасности ИСПДн.

10.4. Список лиц, имеющих доступ к персональным данным, уполномоченных на обработку этих данных и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты персональных данных, утверждается приказом руководителя.

10.5. Сотрудники учреждения, которым доступ к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей (далее – пользователи), для получения доступа к информационной системе направляют письменный запрос на имя ответственного за обеспечение безопасности персональных данных.

10.6. При обнаружении нарушений порядка предоставления персональных данных уполномоченное лицо незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

10.7. Иные требования по обеспечению безопасности информации и средств защиты информации в Учреждении выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти Кемеровской области.

11. Особенности обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных

11.1. Состав информационных систем персональных данных и их характеристика определяется Перечнем информационных систем персональных данных (приложение 3).

11.2. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

11.3. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

11.4. Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством РФ порядке.

11.5. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

11.6. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

11.7. Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает специалист, ответственный за организацию обработки персональных данных в ИСПДн (администратор безопасности ИСПДн).

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

11.8.1. проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

11.8.2. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

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

11.8.4. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

11.8.5. постоянный контроль над обеспечением уровня защищенности персональных данных.

11.9. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:

11.9.1. определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

11.9.2. разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

11.9.3. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

11.9.4. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

11.9.5. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

11.9.6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

11.9.7. учет лиц, допущенных к работе с персональными данными в информационной системе;

11.9.8. контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

11.9.9. разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

11.9.10. описание системы защиты персональных данных.

12. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

12.1. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИСПДн, администратора безопасности ИСПДн и ответственного за организацию обработки персональных данных.

12.2. Сотрудники учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

12.2.1. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним доступ), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами (приказами, распоряжениями), влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник учреждения, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае

причинения его действиями ущерба Учреждению (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

12.2.2. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

12.2.3. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

12.3. Руководитель учреждения за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

13. Заключительные положения

13.1. Настоящее Положение утверждается руководителем и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным.

13.2. Все сотрудники, участвующие в обработке персональных данных с использованием средств автоматизации, должны быть ознакомлены с настоящим Положением под подпись.

Лист ознакомления с
Положением об обработке персональных данных с использованием средств
автоматизации

| Дата ознакомления | ФИО сотрудника, ознакомившегося с документом | Должность сотрудника, ознакомившегося с документом | Подпись сотрудника, ознакомив- шегося с документом |
|----------------------|---|---|--|
| 1 | 2 | 3 | 4 |
| | Антоник Ирина Николаевна | учитель технологии | |
| | Базылев Андрей Павлович | водитель | |
| | Бардакова Любовь Александровна | секретарь | |
| | Божко Ольга Викторовна | учитель русского языка и литературы | |
| | Верхозин Александр Францевич | учитель физической культуры, заместитель директора по БОП | |
| | Верюжеская Татьяна Валентиновна | учитель начальных классов | |
| | Гейнц Наталья Алексеевна | учитель биологии и химии | |
| | Игнатенко Мария Евгеньевна | учитель русского языка, литературы и истории | |
| | Казеннова Ирина Владимировна | учитель физики | |
| | Крюков Андрей Григорьевич | водитель | |
| | Ложкина Екатерина Александровна | учитель математики | |
| | Норова Светлана Анатольевна | учитель начальных классов | |
| | Панкова Регина Ринатовна | учитель начальных классов | |
| | Проценко Андрей Иванович | механик | |
| | Роут Ольга Николаевна | сторож | |
| | Садчикова Виктория Сергеевна | учитель географии, обществознания и права | |
| | Степанова Светлана Александровна | воспитатель | |
| | Сало Наталья Валерьевна | воспитатель, замести- тель директора по ДО | |
| | Сарапкина Рауля Инсафовна | завхоз | |
| | Сухорукова Ольга Борисовна | младший воспитатель | |

Приложение 1
к Положению об обработке
персональных данных с
использованием средств
автоматизации

СОГЛАСИЕ
на обработку персональных данных
(форма для сотрудников)

Я, _____,
(Фамилия Имя Отчество субъекта персональных данных полностью)

основной документ, удостоверяющий личность _____

(вид, номер, сведения о дате выдачи указанного документа и выдавшем его органе)

проживающий по адресу (с указанием индекса): _____

настоящим даю свое согласие МБОУ «Шарапская СОШ» (далее –
Учреждение) в лице ответственного за обработку персональных данных
(далее – Оператор), на обработку персональных данных (см. п.3) на
следующих условиях:

1. Согласие дается мною в целях осуществления трудовых
(договорных) отношений с Учреждением, передачи данных в организации,
указанные в п.4, соблюдения федеральных законов и иных нормативно-
правовых актов Российской Федерации.

2. Настоящее согласие дается на осуществление следующих действий в
отношении моих персональных данных, которые необходимы для
достижения указанных выше целей, совершаемых с использованием средств
автоматизации или без использования таких средств, включая, без
ограничения: сбор, запись, систематизацию, накопление, хранение,
уточнение (обновление, изменение), извлечение, использование, передачу
(предоставление, доступ), обезличивание, блокирование, удаление,
уничтожение моих персональных данных, а также любых иных действий с
учетом действующего законодательства РФ.

3. Типовой перечень персональных данных передаваемых Оператору
на обработку:

- 3.1. фамилия имя отчество;
- 3.2. ИНН;
- 3.3. СНИЛС (№ страхового пенсионного свидетельства);
- 3.4. табельный номер;
- 3.5. пол;
- 3.6. номер, дата трудового договора;
- 3.7. дата рождения;
- 3.8. место рождения;

- 3.9. гражданство;
- 3.10. наименование и степень знания иностранного языка;
- 3.11. образование (среднее общее, начальное профессиональное, среднее профессиональное, высшее, аспирантура, адъюнктура, докторантура);
- 3.12. наименование образовательного учреждения;
- 3.13. наименование, серия, номер, дата выдачи, направление или специальность, код по ОКСО, ОКИН документа об образовании, о квалификации или наличии специальных знаний
- 3.14. профессия (в т.ч. код по ОКПДТР);
- 3.15. стаж работы;
- 3.16. состояние в браке;
- 3.17. состав семьи, с указанием степени родства, фамилии, имени, отчества, года рождения ближайших родственников;
- 3.18. данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);
- 3.19. адрес и дата регистрации;
- 3.20. фактический адрес места жительства;
- 3.21. телефон;
- 3.22. сведения о воинском учете (категория запаса, воинское звание, состав (профиль), полное кодовое обозначение ВУС; категория годности к военной службе, наименование военного комиссариата по месту жительства, состоит на воинском учете, отметка о снятии с учета);
- 3.23. дата приема на работу;
- 3.24. характер работы;
- 3.25. вид работы (основной, по совместительству);
- 3.26. структурное подразделение;
- 3.27. занимаемая должность (специальность, профессия), разряд, класс (категория) квалификации;
- 3.28. ранее занимаемая должность;
- 3.29. должность, занимаемая в порядке совмещения (внутреннего и внешнего);
- 3.30. тарифная ставка (оклад), надбавка, руб.
- 3.31. основание трудоустройства;
- 3.32. личная подпись сотрудника;
- 3.33. фотография;
- 3.34. сведения об аттестации (дата, решение, номер и дата документа, основание);
- 3.35. сведения о повышении квалификации и профессиональной переподготовке (дата начала и окончания обучения, специальность (направление, профессия), наименование, номер, дата документа свидетельствующего о повышении квалификации или переподготовке, основание);
- 3.36. сведения о наградах, поощрениях, почетных званиях (наименование, номер, дата награды);

3.37. сведения об отпусках (вид, период работы, количество дней, дата начала и окончания, основание);

3.38. сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством (наименование льготы, номер, дата выдачи документа, основание);

3.39. сведения об увольнении (основания, дата, номер и дата приказа);

3.40. объем работы, недельная нагрузка;

3.41. сведения о доходах;

3.42. сведения из трудовой книжки, водительского удостоверения, медицинской справки о допуске к управлению автомобиля и подтверждаю, что, давая такое согласие, я действую по своей воле и в своих интересах.

4. Оператор имеет право передавать персональные данные субъекта в Пенсионный Фонд РФ, Федеральную Налоговую Службу РФ, филиалы ПАО Сбербанк РФ, Департамент образования и науки Кемеровской области, Управлению образования администрации Прокопьевского муниципального района, Управлению социальной защиты населения администрации Прокопьевского муниципального района, и иным третьим лицам в соответствии с законодательством Российской Федерации.

5. Субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии с п.7 ст. 14 ФЗ №152 «О персональных данных» от 27.07.2006г.).

6. Настоящее согласие дается до момента прекращения трудовых (договорных отношений) с Учреждением, после чего персональные данные уничтожаются или обезличиваются (за исключением личных дел работников, которые хранятся в специально отведенном для этих целей месте).

7. Согласие может быть отозвано путем направления соответствующего письменного уведомления в адрес Оператора по почте заказным письмом, с уведомлением о вручении, либо вручен лично под расписку представителю Оператора, после чего Оператор обязуется в течение 30 (Тридцати) дней уничтожить, либо обезличить персональные данные Субъекта.

« _____ » _____ 20 _____ г.
(дата)

_____/_____
(подпись) (расшифровка подписи)

ПЕРЕЧЕНЬ
сведений, содержащих персональные данные

1. Сведения, составляющие персональные данные:

- 1.1. Сведения, составляющие персональные данные сотрудников:
 - 1.1.1. фамилия имя отчество;
 - 1.1.2. ИНН;
 - 1.1.3. СНИЛС (№ страхового пенсионного свидетельства);
 - 1.1.4. табельный номер;
 - 1.1.5. пол;
 - 1.1.6. номер, дата трудового договора;
 - 1.1.7. дата рождения;
 - 1.1.8. место рождения;
 - 1.1.9. гражданство;
 - 1.1.10. наименование и степень знания иностранного языка;
 - 1.1.11. образование (среднее общее, начальное профессиональное, среднее профессиональное, высшее, аспирантура, адъюнктура, докторантура);
 - 1.1.12. наименование образовательного учреждения;
 - 1.1.13. наименование, серия, номер, дата выдачи, направление или специальность, код по ОКСО, ОКИН документа об образовании, о квалификации или наличии специальных знаний
 - 1.1.14. профессия (в т.ч. код по ОКПДТР);
 - 1.1.15. стаж работы;
 - 1.1.16. состояние в браке;
 - 1.1.17. состав семьи, с указанием степени родства, фамилии, имени, отчества, года рождения ближайших родственников;
 - 1.1.18. данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);
 - 1.1.19. адрес и дата регистрации;
 - 1.1.20. фактический адрес места жительства;
 - 1.1.21. телефон;
 - 1.1.22. сведения о воинском учете (категория запаса, воинское звание, состав (профиль), полное кодовое обозначение ВУС; категория годности к военной службе, наименование военного комиссариата по месту жительства, состоит на воинском учете, отметка о снятии с учета);
 - 1.1.23. дата приема на работу;
 - 1.1.24. характер работы;
 - 1.1.25. вид работы (основной, по совместительству);

- 1.1.26. структурное подразделение;
- 1.1.27. занимаемая должность (специальность, профессия), разряд, класс (категория) квалификации;
- 1.1.28. ранее занимаемая должность;
- 1.1.29. должность, занимаемая в порядке совмещения (внутреннего и внешнего);
- 1.1.30. тарифная ставка (оклад), надбавка, руб.
- 1.1.31. основание трудоустройства;
- 1.1.32. личная подпись сотрудника;
- 1.1.33. фотография;
- 1.1.34. сведения об аттестации (дата, решение, номер и дата документа, основание);
- 1.1.35. сведения о повышении квалификации и профессиональной переподготовке (дата начала и окончания обучения, специальность (направление, профессия), наименование, номер, дата документа свидетельствующего о повышении квалификации или переподготовке, основание);
- 1.1.36. сведения о наградах, поощрениях, почетных званиях (наименование, номер, дата награды);
- 1.1.37. сведения об отпусках (вид, период работы, количество дней, дата начала и окончания, основание);
- 1.1.38. сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством (наименование льготы, номер, дата выдачи документа, основание);
- 1.1.39. сведения об увольнении (основания, дата, номер и дата приказа);
- 1.1.40. объем работы, недельная нагрузка;
- 1.1.41. сведения о доходах;
- 1.1.42. сведения из трудовой книжки, водительского удостоверения, медицинской справки о допуске к управлению автомобиля.

- 1.2. Сведения, составляющие персональные данные граждан:
 - 1.2.1. фамилия, имя, отчество;
 - 1.2.2. пол;
 - 1.2.3. дата рождения;
 - 1.2.4. место рождения;
 - 1.2.5. семейное положение;
 - 1.2.6. данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);
 - 1.2.7. адрес и дата регистрации;
 - 1.2.8. фактический адрес жительства;
 - 1.2.9. контактные телефоны;
 - 1.2.10. СНИЛС;
 - 1.2.11. ИНН;
 - 1.2.12. место работы;
 - 1.2.13. профессия, должность;

- 1.2.14. социальный статус;
- 1.2.15. категория льготы.

2. Основания обработки персональных данных

- 2.1. Конституция Российской Федерации;
- 2.2. Гражданский кодекс Российской Федерации;
- 2.3. Трудовой кодекс Российской Федерации
- 2.4. Налоговый Кодекс Российской Федерации;
- 2.5. Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- 2.6. Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
- 2.7. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;
- 2.8. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных»;
- 2.9. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- 2.10. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- 2.11. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- 2.12. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- 2.13. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- 2.14. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- 2.15. Приказ Минздравсоцразвития России от 12.04.2011 № 302н (ред. от 15.05.2013) «Об утверждении перечней вредных и (или) опасных производственных факторов и работ, при выполнении которых проводятся обязательные предварительные и периодические медицинские осмотры (обследования), и Порядка проведения обязательных предварительных и периодических медицинских осмотров (обследований) работников, занятых на тяжелых работах и на работах с вредными и (или) опасными условиями труда»;
- 2.16. Федеральный закон от 29.12.2012г. № 273-ФЗ «Об образовании в Российской Федерации».

Приложение 3
к Положению об обработке
персональных данных
с использованием средств
автоматизации

ПЕРЕЧЕНЬ
информационных систем персональных данных (ИСПДн)

| № п/п | Наименование ИСПДн | Наименование и адрес объекта |
|--------------|--|---|
| 1 | 2 | 3 |
| 1 | АИС «Электронная школа 2.0» | https://ruobr.ru |
| 2 | АИС «Образование Кемеровской области» | http://mon.kuz-edu.ru |
| 3 | АИС «ДОУ-банк» | https://dou.ruobr.ru |
| 4 | Областной центр мониторинга качества образования | http://ocmko.ru |
| 5 | Информационный портал «Всероссийские проверочные работы» | https://vpr.statgrad.org |
| 6 | Официальный сайт МБОУ «Шарапская СОШ» | http://sharap-prk.edusite.ru |
| | | |
| | | |
| | | |