РАССМОТРЕНО
на административном совещании
05.11.2019 г.

УТВЕРЖДЕНО
Директор
МОАУ «СОШ № 11 г. Орска»
_____ **Е.Н. Николаюк**

Приказ № 210 от 20.11.2019 г.

ПОЛОЖЕНИЕ
о персональных данных работников МОАУ «СОШ № 11 г. Орска»

1. Термины и определения.

В целях настоящего положения используются следующие основные понятия:

1) персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (**субъекту персональных данных** (**работнику**);

2) оператор персональных данных (**оператор** (**МОАУ «СОШ № 11 г. Орска»**) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) 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;

4) автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) 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;

9) обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2. Состав персональных данных.

2.1. В состав персональных данных работника включаются:

1) сведения о фактах, событиях и обстоятельствах частной жизни работника, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2) служебные сведения, а также иные сведения, связанные с профессиональной деятельностью работника, в том числе сведения о поощрениях и о дисциплинарных взысканиях.

2.2. К персональным данным Работника относятся:

1) фамилия, имя, отчество;
2) дата рождения;
3) гражданство;
4) семейное положение;
5) данные о членах семьи (степень родства, Ф. И. О., год рождения, паспортные данные, включая прописку и место рождения);
6) фактическое место проживания;
7) разрешение на временное проживание или вид на жительство для иностранных граждан;
8) контактная информация;
9) данные об образовании (реквизиты дипломов/иных документов);
10) данные о приобретенных специальностях;
11) трудовая книжка;
12) паспорт или иной документ, удостоверяющий личность;
13) уведомление о регистрации в системе индивидуального (персонифицированного) учёта формы № АДИ-РЕГ;
14) свидетельство о постановке на учёт в налоговый орган и присвоении ИНН;
15) документы воинского учёта;
16) личная карточка работника ф. Т-2;
17) анкета (личный листок по учёту кадров);
18) автобиография;
19) справка об отсутствии судимости или факта уголовного преследования;
20) справка о прохождении предварительного медосмотра;
21) личная медицинская книжка;
22) заявление о приёме на работу;
23) письменное согласие на обработку персональных данных;
24) трудовой договор;
25) договоры, заключаемые между оператором и субъектом персональных данных;
26) приказы о приёме на работу, об увольнении, а также о переводе на другую должность;
27) данные о текущей трудовой деятельности (дата начала трудовой деятельности, кадровые перемещения, оклады и их изменения, сведения о поощрениях, данные о повышении квалификации и т. п.).

3. Общие положения.

3.1. Настоящим Положением регулируются отношения, связанные с обработкой персональных данных, осуществляемой МОАУ «СОШ № 11 г. Орска» и физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

3.2. Настоящее Положение устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных.

3.3. Настоящее Положение разработано в целях обеспечения защиты прав и свобод субъекта персональных данных при обработке его персональных данных, в том числе от несанкционированного доступа, неправомерного их использования или утраты.

3.4. Настоящее Положение разработано в соответствии со следующими нормативными правовыми актами:

- Трудовой кодекс Российской Федерации (ст. 86-90);

- Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями и дополнениями);

- Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» (в ред. Федеральных законов от 25.11.2009г. № 266-ФЗ, от 27.12.2009 г. № 363-ФЗ, от 28.06.2010 г. № 123-ФЗ, от 27.07.2010 г. № 204-ФЗ, от 27.07.2010 г. № 227-ФЗ, от 29.11.2010 г. № 313-ФЗ, от 23.12.2010 г. № 359-ФЗ, от 04.06.2011 г. № 123-ФЗ, от 25.07.2011 г. № 261-ФЗ, от 05.04.2013 г. № 43-ФЗ, от 23.07.2013 г. № 205-ФЗ, от 21.12.2013 г. № 363-ФЗ, от 04.06.2014 г. № 142-ФЗ, от 21.07.2014 г. № 216-ФЗ, от 21.07.2014 г. № 242-ФЗ, от 03.07.2016 г. № 231-ФЗ, от 22.02.2017 г. № 16-ФЗ, от 01.07.2017 г. № 148-ФЗ, от 29.07.2017 г. № 223-ФЗ, от 31.12.2017 г. № 498-ФЗ);

- Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

- рекомендации Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31.07.2017 г. «Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

3.5. Персональные данные работников относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом. По истечении срока хранения бумажные носители, содержащие персональные данные работников, сдаются в архив.

3.6. Оператор, получив доступ к персональным данным, обязан соблюдать конфиденциальность персональных данных – не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3.7. Настоящее Положение утверждается и вводится в действие приказом директора и является обязательным для исполнения всеми должностными лицами МОАУ «СОШ № 11 г. Орска», имеющими доступ к персональным данным работников.

4. Цели сбора персональных данных.

4.1. К целям обработки персональных данных оператором относятся:

- исполнение требований налогового законодательства по вопросам исчисления и уплаты налога на доходы физических лиц и единого социального налога, пенсионного законодательства при формировании и передаче в ПФР персонифицированных данных о каждом получателе доходов, которые учитываются при начислении взносов на обязательное пенсионное страхование;

- заполнение первичной статистической документации в соответствии с трудовым, налоговым законодательством и иными федеральными законами;

- формирование кадрового резерва оператора;

- учёт сотрудников, награждённых государственными наградами Российской Федерации, представленных к награждению.

4.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

4.3. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность

по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

5. Объём и категории обрабатываемых персональных данных, категории субъектов персональных данных.

5.1. Содержание и объём обрабатываемых персональных данных соответствуют заявленным целям обработки.

5.2. К категориям персональных данных, обрабатываемых оператором, относятся:

- работники оператора, бывшие работники, а также родственники работников;
- педагогические работники.

6. Порядок и условия обработки персональных данных.

6.1. Оператор осуществляет обработку персональных данных с использованием средств автоматизации или без использования таких средств.

6.2. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

6.3. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.4. Оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

6.5. Документы, содержащие персональные данные работника, создаются путём:

а) копирования оригиналов;

б) внесения сведений в учётные формы (на бумажных и электронных носителях);

в) получения оригиналов необходимых документов (трудовая книжка, анкета (личный листок по учёту кадров), автобиография, медицинское заключение и др.).

6.6. Сведения, содержащие персональные данные работника, включаются в его личное дело, личную карточку формы Т-2, а также содержатся на электронных носителях информации, доступ к которым разрешён лицам, непосредственно использующим персональные данные работника в служебных целях. Перечень должностных лиц, имеющих право доступа к персональным данным работников, определён в пункте 7.1. настоящего Положения.

6.7. Персональные данные должны быть получены лично у работника. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлён об этом заранее и от него должно быть получено письменное согласие.

6.8. Обработка специальных категорий персональных данных, касающихся национальной принадлежности, состояния здоровья, допускается в случае, если субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных.

6.9. Хранение персональных данных работников осуществляется следующим образом:

- персональные данные, включённые в состав личных дел, хранятся в запертом металлическом сейфе, установленном на рабочем месте секретаря. Персональные данные, содержащиеся на электронных носителях информации, хранятся в персональном компьютере секретаря;

- трудовые книжки, документы воинского учёта, личные медицинские книжки, личные дела, личные карточки формы Т-2 хранятся в запертом металлическом сейфе.

Доступ к электронным базам данных, содержащим персональные данные работников, обеспечивается с помощью установления паролей.

Пароли устанавливаются на каждом персональном компьютере индивидуально.

Доступ к электронным и бумажным носителям, содержащим персональные данные субъекта, строго ограничен кругом лиц, определённых в пункте 7.1 настоящего Положения.

7. Доступ к персональным данным работника.

7.1. Внутренний доступ (работники МОАУ «СОШ № 11 г. Орска»).

Доступ к персональным данным работников имеют следующие должностные лица, непосредственно использующие их в служебных целях:

1) директор;
2) заместители директора;
3) секретарь;
4) должностное лицо, ответственное за работу по оформлению и информационному наполнению сайта образовательной организации.

7.1.1. Уполномоченные лица имеют право получать только те персональные данные работника, которые необходимы им для выполнения конкретных функций в соответствии с должностной инструкцией. Все остальные работники имеют право на получение полной информации только о своих персональных данных и их обработке.

7.1.2. Получение сведений о персональных данных работников третьей стороной разрешается только при наличии заявления с указанием конкретных персональных данных и целей, для которых они будут использованы, а также письменного согласия работника, персональные данные которого затребованы.

7.1.3. Получение персональных данных работника третьей стороной без его письменного согласия возможно в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных законом.

7.2. Внешний доступ (другие организации и граждане).

Сообщение сведений о персональных данных работников другим организациям и гражданам разрешается при наличии письменного согласия работника и заявления, подписанного руководителем организации либо гражданином, запросившим такие сведения.

7.2.1. Предоставление сведений о персональных данных работников без соответствующего их согласия возможно в следующих случаях:

а) в целях предупреждения угрозы жизни и здоровью работника;

б) при поступлении официальных запросов в соответствии с положениями Федерального закона «Об оперативно-розыскных мероприятиях»;
в) при поступлении официальных запросов из налоговых органов, органов Пенсионного Фонда России, органов Федерального социального страхования, судебных органов.

7.2.2. Работник, о котором запрашиваются сведения, должен быть уведомлён о передаче его персональных данных третьим лицам, за исключением случаев, когда такое уведомление невозможно в силу форс-мажорных обстоятельств, а именно: стихийных бедствий, аварий, катастроф.

7.2.3. Запрещается передача персональных данных работника в коммерческих целях без его согласия.

7.2.4. Передача сведений, содержащих персональные данные работника, его представителю осуществляется только при наличии надлежащим образом оформленной Доверенности представителя.

8. Меры по обеспечению безопасности персональных данных, их защита от актуальных угроз и опасности утраты.

8.1. Под актуальными угрозами безопасности или опасностью утраты персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

8.2. Защита персональных данных представляет собой предупреждение нарушения доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечение безопасности информации в процессе управленческой и производственной деятельности организации.

8.3. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры для защиты персональных данных, в частности:

8.3.1. В МОАУ «СОШ № 11 г. Орска» устанавливается необходимость обеспечения 3-го уровня защищённости персональных данных при их обработке в информационной системе, так как для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора.

8.3.2. Для обеспечения 3-го уровня защищённости персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

- назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

8.3.3. **«Внутренняя защита»:**

1. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и сотрудниками организации.

Для обеспечения внутренней защиты персональных данных необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- наличие режима организации учёта и сохранности персональных данных:
  - ведение журнала учёта передачи носителей информации (USB-флеш-накопитель);
  - хранение носителей информации (USB-флеш-накопитель) в запертом металлическом сейфе или шкафу;
  - учёт машинных носителей персональных данных;
- своевременное обновление баз данных антивирусной защиты;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками организации;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
- воспитательная и разъяснительная работа с работникам организации по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

2. Защита персональных данных на электронных носителях. Все папки, содержащие персональные данные, должны быть защищены паролем.

3. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищённости информационных систем персональных данных.

8.3.4. **«Внешняя защита»:**

1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение и др.

2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к организации: посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов.

3. Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

- порядок приёма, учёта и контроля деятельности посетителей;
- пропускной режим организации;
- технические средства охраны, сигнализация;
- требования к защите информации при интервьюировании и собеседованиях.

9. Актуализация, исправление, удаление и уничтожение персональных данных.

9.1. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения.

В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные.

Оператор обязан уведомить субъекта персональных данных или его представителя о внесённых изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым эти персональные данные этого субъекта были переданы.

9.2. Оператор обязан прекратить обработку персональных данных или обеспечить прекращение обработки персональных данных лицом, действующим по поручению оператора:

- в случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, в срок, не превышающий трёх дней с даты этого выявления;
- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператором;
- в случае достижения цели обработки персональных данных и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществлялась другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработки персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

10. Права и обязанности по защите персональных данных.

10.1. **Субъект персональных данных имеет право** на получение полной информации, касающейся обработки его персональных данных.

10.2. Данные сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

10.3. Субъект персональных данных вправе получать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

10.4. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

10.5. **Оператор персональных данных вправе** отстаивать свои интересы в суде.

10.6. Предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.).

10.7. Отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством.

10.8. Использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством.

10.9. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных субъекта.

10.10. **Оператор обязан** обеспечить защиту персональных данных субъекта от неправомерного их использования или утраты в порядке, установленном законодательством РФ.

10.11. Оператор, получив доступ к персональным данным, обязан соблюдать конфиденциальность персональных данных – не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

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

11.1. Работники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

12. Заключительные положения.

12.1. Настоящее Положение вступает в силу с момента его утверждения директором МОАУ «СОШ № 11 г. Орска» и действует бессрочно, до замены его новым Положением.

12.2. Все изменения в Положение вносятся приказом директором МОАУ «СОШ № 11 г. Орска».

12.3. Все должностные лица МОАУ «СОШ № 11 г. Орска», имеющие доступ к персональным данным работников, должны быть ознакомлены с настоящим Положением под роспись.