Приложение
к приказу от «___» _____ 20__ г. № ____

ПОЛИТИКА
МАОУ «ГИМНАЗИЯ № 1 Г.БЛАГОВЕЩЕНСКА»
В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящая политика (далее - Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон о ПДн) и является основополагающим внутренним регулятивным документом Муниципального автономного общеобразовательного учреждения «Гимназия № 1 города Благовещенска» (далее - образовательная организация или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является образовательная организация.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в образовательной организации, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных образовательной организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Если в отношениях с образовательной организацией участвуют наследники (правопреемники) и (или) представители субъектов ПДн, то образовательная организация становится оператором ПДн лиц, представляющих указанных субъектов. Положения Политики и другие внутренние регулятивные документы Ооразовательной организации распространяются на случаи обработки и защиты ПДн наследников (правопреемников) и (или) представителей субъектов ПДн, даже если эти лица во внутренних регулятивных документах прямо не упоминаются, но фактически участвуют в правоотношениях с образовательной организацией.

2. Основания обработки и состав персональных данных, обрабатываемых в образовательной организации

2.1. Обработка ПДн в образовательной организации осуществляется в связи с выполнением законодательно возложенных на образовательную организацию функций, определяемых:

1) Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

2) Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации»;

3) Федеральным законом от 25.12.2008 № 273-ФЗ «О противодействии коррупции»;

6) иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка ПДн в образовательной организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых образовательная организация выступает в качестве работодателя (гл. 14 Трудового кодекса Российской Федерации), в связи с реализацией образовательной организацией своих прав и обязанностей как юридического лица.

2.2. В рамках осуществления функций предоставления общедоступного и бесплатного среднего общего образования; дополнительного образования в муниципальных образовательных организациях ПДн обрабатываются образовательной организацией при приеме заявлений и зачислении детей в муниципальные образовательные учреждения, реализующие основные общеобразовательные и дополнительные образовательные программы.

2.3. В связи с трудовыми и иными непосредственно связанными с ними отношениями, в которых образовательная организация выступает в качестве работодателя, обрабатываются ПДн лиц, претендующих на трудоустройство в образовательной организации, работников образовательной организации (далее - Работники) и бывших Работников.

2.4. В связи с реализацией своих прав и обязанностей как юридического лица, образовательной организацией обрабатываются ПДн физических лиц, являющихся контрагентами (возможными контрагентами) образовательной организации по гражданско-правовым договорам, ПДн руководителей, членов коллегиальных исполнительных органов и представителей юридических лиц, ПДн иных физических лиц, представленные участниками закупки, а также граждан, письменно обращающихся в образовательную организацию по вопросам его деятельности.

2.5. ПДн получаются и обрабатываются образовательной организацией на основании федеральных законов и иных нормативных правовых актов Российской Федерации, а в необходимых случаях - при наличии письменного согласия субъекта ПДн.

2.5.1. В целях обеспечения прав Субъектов ПДн Оператор при обработке ПДн Субъектов ПДн обязан соблюдать следующие принципы:

обработка ПДн должна осуществляться на законной и справедливой основе;

обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн;

не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

обработке подлежат только ПДн, которые отвечают целям их обработки;

содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки;

при обработке ПДн должны быть обеспечены точность ПДн, 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;

хранение ПДн должно осуществляться в форме, позволяющей определить Субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является Субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.5.2. В соответствии со ст. 6 ФЗ-152 «О Персональных данных» Оператор при обработке ПДн должен соблюдать следующие общие требования:

2.5.2.1. Обработка ПДн осуществляется только с согласия Субъекта ПДн на обработку его ПДн.

Оператор имеет право обрабатывать ПДн Субъектов ПДн только с их письменного согласия в следующих случаях, предусмотренных Федеральным законом №152-ФЗ «О персональных данных»:

при передаче обработки ПДн третьему лицу;

при обработке специальных категорий ПДн;

при обработке биометрических ПДн;

при включении ПДн субъекта в общедоступные источники ПДн (в том числе справочники, адресные книги и Т.П.);

при необходимости трансграничной передачи ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав Субъектов ПДн;

в случае принятия решений, порождающих юридические последствия в отношении Субъекта ПДн или иным образом затрагивающих его права и законные интересы на основании исключительно автоматизированной обработки его ПДн;

в случае недееспособности Субъекта ПДН, когда за него согласие на обработку ПДн Субъекта дает законный представитель Субъекта ПДн.

Письменное согласие Субъекта ПДн на обработку своих ПДн должно включать в себя:

фамилию, имя, отчество, адрес Субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

фамилию, имя отчество, адрес представителя Субъекта ПДн, 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 ПДн);

наименование или фамилию, имя, отчество адрес Оператора, получающего согласие Субъекта ПДн;

цель обработки ПДн;

перечень ПДн, на обработку которых дается согласие Субъекта ПДн;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка будет поручена такому лицу;

перечень действий с ПДН, на совершение которых дается согласие, общее описание используемых Оператором способов обработки ПДн;

срок, в течение которого действует согласие Субъекта ПДн, а также порядок его отзыва, если иное не установлено федеральным законом;

подпись Субъекта ПДн.

Равнозначным содержащему собственноручную подпись Субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Формы согласия на обработку ПДн разрабатываются Оператором самостоятельно и утверждаются его локальным актом.

Согласие на обработку ПДн работника и Обязательство о неразглашении им конфиденциальной информации (персональных данных), которая будет ему вверена в целях исполнения своих должностных обязанностей, выдаются работнику сразу при приеме его на работу и регистрируются в «Журнале учета Согласий на обработку персональных данных работников и Обязательств о неразглашении конфиденциальной информации (персональных данных) не содержащей сведений, составляющих государственную тайну».

Согласие на обработку ПДн может быть отозвано Субъектом ПДн в любое время на основании его письменного заявления, поданного на имя руководителя образовательной организации. В случае отзыва Субъектом ПДн согласия на обработку его ПДн Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если Обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение ПДн более не требуется для целей обработки ПДН, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в

срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн, иным соглашением между Оператором и Субъектом ПДн либо если Оператор не вправе осуществлять обработку ПДн без согласия Субъекта ПДн на основаниях, предусмотренных законодательством Российской Федерации.

В случае отсутствия возможности уничтожения ПДн в течение указанного срока, Оператор осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

В случае получения согласия на обработку ПДн от представителя Субъекта ПДн полномочия данного представителя на дачу согласия от имени Субъекта ПДн проверяются Оператором.

2.5.2.2. Обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей.

2.5.2.3. Обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве.

2.5.2.4. Обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является Субъект ПДн, а также для заключения договора по инициативе Субъекта ПДн или договора, по которому Субъект ПДн будет являться выгодоприобретателем или поручителем.

2.5.2.5. Обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов Субъекта ПДн, если получение согласия Субъекта ПДн невозможно.

2.5.2.6. Обработка ПДн необходима для осуществления прав и законных интересов Оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы Субъекта ПДн.

2.5.2.7. Обработка ПДн осуществляется в статистических или иных исследовательских целей при условии обязательного обезличивания ПДн, за исключением случаев обработки ПДн в маркетинговых целях.

2.5.2.8. Осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральными законами.

2.5.3. Оператор не имеет права получать и обрабатывать специальные категории ПДн Субъекта ПДн, касающихся его расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состоянии здоровья, интимной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за

исключением случаев, предусмотренных Трудовым кодексом Российской Федерации и иными федеральными законами, а также в случаях, если:

Субъект ПДн дал согласие в письменной форме на обработку своих ПДн;

ПДн сделаны общедоступными Субъектом ПДн;

обработка ПДн осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов Субъекта ПДн либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия Субъекта ПДн невозможно;

обработка ПДн осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медикосоциальных услуг при условии, что обработка ПДн осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

обработка ПДн необходима для установления или осуществления прав Субъекта ПДн или третьих лиц, а равно и в связи с осуществлением правосудия;

обработка ПДн осуществляется в соответствии с законодательством Российской Федерации о безопасности, о противодействии терроризму, о противодействии коррупции, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации;

по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации Оператор, как работодатель, вправе получать и обрабатывать данные о частной жизни Субъекта ПДн только с его письменного согласия. Обработка специальных категорий ПДн должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась их обработка, если иное не установлено федеральным законом.

2.6. В целях исполнения возложенных на образовательную организацию функций образовательная организация в установленном порядке вправе поручить обработку ПДн третьим лицам.

В договоры с лицами, которым образовательная организация поручает обработку ПДп, включаются условия, обязывающие таких лиц соблюдать предусмотренные законодательством требования к обработке и защите ПДн.

2.7. Образовательная организация предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПДн.

2.8. В образовательной организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в образовательной организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся образовательной организацией ПНд уничтожатся или обезличиваются.

2.9. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Образовательная организация принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

2.10. Состав ПДн.

2.10.1 Объем и содержание обрабатываемых в образовательной организации ПДн определяется в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом №152-ФЗ «О персональных данных» и иными федеральными законами и нормативными актами.

2.10.2 В состав ПДн Субъекта ПДн входят сведения, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства и другая информация, позволяющая идентифицировать Субъекта ПДн и получить дополнительную информацию о нем и его родственниках.

2.10.3. В состав ПДн обучающегося, в частности, входят:

фамилия, имя, отчество;

пол;

дата и место рождения;

гражданство;

сведения свидетельства о рождении;

паспортные данные (иного документа, удостоверяющего личность) (для лиц, старше 14 лет);

адрес регистрации и фактического места жительства;

личная фотография;

контактный телефон;

отметки об успеваемости;

данные медицинской карты;

сведения о воинском учете (для лиц, старше 14 лет);

сведения, дающие право на социальные льготы (сирота, инвалид и т.д.);

иные сведения, необходимые для целей Оператора в рамках действующего законодательства.

2.10.4. В состав ПДн родителя (законного представителя) обучающегося, в частности, входят:

фамилия, имя, отчество;

гражданство;

паспортные данные (иного документа, удостоверяющего личность);

сведения свидетельства о рождении ребенка;

адрес регистрации и фактического места жительства;

контактная информация (номер(а) телефона(ов), адрес(а) электронной почты);

данные документа, подтверждающего права законного представителя;

данные документов, предоставляющих право на получение компенсаций и льгот, связанных с обучением, присмотром и уходом за ребенком в образовательной организации и т.п.;

иные сведения, необходимые для целей Оператора в рамках действующего законодательства.

2.10.5. В состав ПДн Работника, в частности, входят:

фамилия, имя, отчество;

пол;

дата и место рождения;

предыдущая фамилия;

сведения о семейном положении и о составе семьи;

гражданство;

ИНН;

номер страхового свидетельства государственного пенсионного страхования;

личная фотография;

сведения медицинского характера (результаты медицинского обследования на предмет осуществления трудовых функций);

паспортные данные (иного документа, удостоверяющего личность);

адрес регистрации и фактического места жительства;

контактная информация (номер(а) телефона(ов), адрес(а) электронной почты);

видео изображения;

сведения об образовании (о дополнительном образовании), специальности;

сведения о повышении квалификации, профессиональной переподготовке и т.п.;

сведения о занимаемой должности;

сведения о трудовом и общем стаже;

сведения о поощрениях, наградах, званиях, ученой(ых) степени(ей);

сведения о социальных льготах;

сведения о наличии/отсутствии судимости;

сведения о воинском учете;

сведения, содержащиеся в рекомендациях, характеристиках;

сведения о посещении семинаров, конференций, тренингов;

сведения, входящие в научные работы, в «Личный листок по учету кадров», в трудовую книжку, в материалы аттестационных комиссий, в приказы;

анкетные данные, заполненные работником при поступлении на работу (резюме);

сведения о заработанной плате;

иные сведения, необходимые для целей Оператора в рамках действующего законодательства.

2.11. Документы ПДн.

2.11.1. К ПДн относится документированная информация, содержащаяся в конкретных документах. Документы, содержащие ПДн Субъектов ПДн:

трудовой договор;

приказы по личному составу;

трудовая книжка;

личное дело;

личная карточка сотрудника (Т 2);

паспорт (иной документ, удостоверяющий личность);

ИНН;

страховое свидетельство государственного пенсионного страхования;

документы воинского учета для военнообязанных и лиц, подлежащих призыву на военную службу;

документы об образовании, квалификации или наличии специальных знаний;

иные документы (анкеты, результаты опросов, тестов, справки, резюме, рекомендации, характеристики, грамоты и др.);

материалы служебных проверок, расследований, аттестационных комиссий;

документы о составе семьи;

медицинские справки о состоянии здоровья;

документы о состоянии здоровья Субъекта ПДн (сведения об инвалидности и т.п.), а также о состоянии здоровья детей, родителей и других близких родственников Субъекта ПДн, когда с наличием таких документов связано предоставление каких-либо гарантий и компенсаций;

документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством;

документы о беременности и возрасте детей для предоставления матери (отцу, иным родственникам) установленных законом условий труда, гарантий, компенсаций;

документы, необходимые для трудоустройства иностранного гражданина (согласно главе 50.1 ТК РФ);

справка об отсутствии судимости;

документ, содержащий сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также сведения о доходах, расходах, об имуществе и обязательствах имущественного характера своих супруги (супруга) и несовершеннолетних детей;

иные документы, содержащие ПДн Субъекта ПДн.

2.11.2. Документы, содержащие ПДн создаются путем:

копирования оригиналов;

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

получения оригинала необходимых документов (трудовая книжка, медицинское заключение и др.)

2.12. ПДн Субъектов ПДн и документы, указанные в пунктах 2.10.3, 2.10.4., 2.11 настоящей Политики, являются конфиденциальными и не могут быть использованы Оператором или иным лицом в личных целях. Режим конфиденциальности снимается в случаях их обезличивания либо по истечении сроков хранения, если иное не определено законом.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в образовательной организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн образовательная организация руководствуется следующими принципами:

1) законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

2) системность: обработка ПДн в образовательной организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3) комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах образовательной организации (далее - ИС) и других имеющихся в образовательной организации систем и средств защиты;

4) непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

5) своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

6) преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в образовательной организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

7) персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

8) минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

9) гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных образовательной организации (далее - ИСПДн), а также объема и состава обрабатываемых ПДн;

10) открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн образовательной организации (далее - СЗПДн) не дают возможности преодоления имеющихся в образовательной организации систем защиты возможными нарушителями безопасности ПДн;

11) научная обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

12) специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

13) эффективность процедур отбора кадров и выбора контрагентов: кадровая политика образовательной организации предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах образовательной организации до заключения договоров;

14) наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

15) непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

4. Доступ к обрабатываемым персональным данным

4.1. Доступ к обрабатываемым в образовательной организации ПДн имеют лица, уполномоченные приказом образовательной организации, лица, которым образовательная организация поручила обработку ПДн, в т.ч. на основании заключенного договора, а также лица, чьи ПДн подлежат обработке.

4.2. В целях разграничения полномочий при обработке ПДн полномочия по реализации каждой определенной законодательством функции образовательной организации закрепляются за соответствующими структурными подразделениями образовательной организации.

Доступ к ПДн, обрабатываемым в ходе реализации полномочий, закрепленных за конкретным структурным подразделением образовательной организации, могут иметь только Работники этого структурного подразделения. Работники допускаются к ПДн, связанным с деятельностью другого структурного подразделения, только для чтения и подготовки обобщенных материалов в части вопросов, касающихся структурного подразделения этих Работников.

4.3. Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов образовательной организации.

Допущенные к обработке ПДн Работники под роспись знакомятся с документами образовательной организации, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.

4.4. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым образовательной организацией, устанавливается в соответствии с законодательством и определяется внутренними регулятивными документами образовательной организации.

5. Реализуемые требования к защите персональных данных

5.1. Образовательная организация принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Законом о ПДн и принятыми в соответствии с ним нормативными правовыми актами, для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

5.2. Состав указанных в пункте 5.1 Политики мер, включая их содержание и выбор средств защиты ПДн, определяется, а внутренние регулятивные документы об обработке и защите ПДн утверждаются (издаются) образовательной организацией исходя из требований:

Закона о ПДн;

главы 14 Трудового кодекса Российской Федерации;

постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн»;

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

постановления Правительства Российской Федерации РФ от 6 июля 2008г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

иных нормативных правовых актов Российской Федерации об обработке и защите ПДн.

5.3. В предусмотренных законодательством случаях обработка ПДн осуществляется образовательной организацией с согласия субъектов ПДн.

Образовательной организацией производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

5.4. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше чем этого требуют цели обработки ПДн, если срок хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

5.5. Образовательной организацией осуществляется ознакомление работников образовательной организации, непосредственно осуществляющих обработку ПДн, с положениями законодательства о ПДн, в том числе требованиями к защите ПДн, Политикой и иными внутренними регулятивными документами по вопросам обработки ПДн, и (или) обучение указанных работников по вопросам обработки и защиты ПДн.

5.6. При обработке ПДн с использованием средств автоматизации образовательной организацией, в частности, применяются следующие меры:

1) назначается ответственный за организацию обработки ПДн, определяется его компетенция;

2) утверждаются (издаются) внутренние регулятивные документы по вопросам обработки и защиты ПДн, в том числе устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;

3) осуществляется внутренний контроль и (или) аудит соответствия обработки ПДн Закону о ПДн и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, Политике и внутренним регулятивным документам образовательной организации;

4) проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Закона о ПДн, определяется соотношение указанного вреда и принимаемых образовательной организацией мер, направленных на обеспечение исполнения обязанностей, предусмотренных Законом о ПДн.

5.7. Обеспечение безопасности ПДн в образовательной организации при их обработке в ИСПДн достигается в образовательной организации, в частности, путем:

1) определения угроз безопасности ПДн. Тип актуальных угроз безопасности ПДн и необходимый уровень защищенности ПДн определяются в соответствии с требованиями законодательства и с учетом проведения оценки возможного вреда;

2) определения в установленном порядке состава и содержания мер по обеспечению безопасности ПДн, выбора средств защиты информации. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности ПДн, а также с учетом экономической целесообразности образовательной организацией могут разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности ПДн. В этом случае в ходе разработки СЗПДн проводится обоснование применения компенсирующих мер для обеспечения безопасности ПДн;

3) применения организационных и технических мер по обеспечению безопасности ПДн, необходимых для выполнения требований к защите ПДн, обеспечивающих определенные уровни защищенности ПДн, включая применение средств защиты информации, прошедших процедуру оценки соответствия, когда применение таких средств необходимо для нейтрализации актуальных угроз.

В образовательной организации, в том числе, осуществляются:

оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;

учет машинных носителей ПДн, обеспечение их сохранности;

обнаружение фактов несанкционированного доступа к ПДн и принятие соответствующих мер;

восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

установление правил доступа к обрабатываемым ПДн, а также обеспечение регистрации и учета действий, совершаемых с ПДн;

контроль за принимаемыми мерами по обеспечению безопасности ПДн, уровня защищенности ИСПДн.

5.8. Обеспечение защиты ПДн в образовательной организации при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:

1) обособления ПДн от иной информации;

2) недопущения фиксации на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;

3) использования отдельных материальных носителей для обработки каждой категории ПДн;

4) принятия мер по обеспечению раздельной обработки ПДн при несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн;

5) соблюдения требований к:

раздельной обработке зафиксированных на одном материальном носителе ПДн и информации, не относящейся к ПДн;

уточнению ПДн;

уничтожению или обезличиванию части ПДн;

использованию типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн;

ведению журналов, содержащих ПДн, необходимых для выдачи однократных пропусков субъектам ПДн в занимаемые образовательной организацией здания и помещения;

хранению ПДн, в том числе к обеспечению раздельного хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

6. Права и обязанности субъекта персональных данных

6.1. Субъект ПДн имеет право:

получать полную информацию о своих ПДН, а также о сведениях, переданных Оператором о Субъекте ПДн третьей стороне;

иметь свободный бесплатный доступ к своим ПДн, включая право на безвозмездное получение копий любой записи, содержащей его ПДн. Сведения о наличии ПДн должны быть предоставлены Субъекту ПДн в доступной форме, и они не должны содержать ПДн, относящиеся к другим Субъектам ПДн. Доступ к своим ПДн предоставляется Субъекту ПДн или его представителю Оператором при личном обращении, либо при получении запроса;

получать сведения об Операторе, о месте его нахождения, о наличии у Оператора сведений о ПДн, относящихся к соответствующему Субъекту ПДн;

требовать от Оператора уточнения, исключения или исправления своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являющихся необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

при отказе исключить или исправить его ПДн, заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия, а при отклонении Оператором указанного обращения (несогласия), обжаловать действия Оператора в порядке, предусмотренном законодательством Российской Федерации;

требовать извещения Оператором всех лиц, которым ранее были сообщены неверные или неполные ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях;

обжаловать в уполномоченный орган по защите прав Субъектов ПДн или в судебном порядке неправомерные действия или бездействия Оператора при обработке и защите его ПДн.

6.2. В целях обеспечения достоверности своих ПДн Субъект ПДн обязан:

предоставлять Оператору полные достоверные данные о себе;

незамедлительно сообщать Оператору об изменении своих персональных данных.

6.3. Право Субъекта ПДн на доступ к своим ПДн ограничивается в случае, если:

обработка ПДн, в том числе ПДн, полученных в результате оперативно-розыскной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

обработка ПДн осуществляется органами, осуществившими задержание Субъекта ПДн по подозрению в совершении преступления, либо предъявившими Субъекту ПДн обвинение по уголовному делу, либо применившими к Субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПДн;

предоставление ПДн нарушает права и законные интересы третьих лиц.

6.4. Решение, порождающее юридические последствия в отношении Субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия Субъекта ПДн в письменной форме или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов Субъекта ПДн.