

УТВЕРЖДАЮ

Директор МБОУ «СОШ № 9»

М.П. Мачнева

«30» декабря 2015 года



ПОЛОЖЕНИЕ
о защите персональных данных
в Муниципальном бюджетном общеобразовательном учреждении
г.Владимира
«Средняя общеобразовательная школа № 9»

ОБЩИЕ ПОЛОЖЕНИЯ

1. Назначение и область распространения

- 1.1 Положением о защите персональных данных (далее – Положение) регулируются отношения, связанные с обработкой персональных данных, осуществляемой Муниципальным бюджетным общеобразовательным учреждением г.Владимира «Средняя общеобразовательная школа № 9» (далее – Школа) 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.
- 1.2 Положение разработано с целью обеспечения защиты прав и свобод работников Школы и иных граждан при обработке их персональных данных.
- 1.3 Действие Положения распространяется на отношения, возникающие при обработке, хранении и защите персональных данных работников, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.
- 1.4 Выполнение Положения обязательно для всех работников Школы, должностные обязанности которых предусматривают обработку и защиту персональных данных.

НОРМАТИВНЫЕ ССЫЛКИ. ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

1. Положение разработано в соответствии с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", постановлением Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", нормативных актов ФСТЭК и ФСБ России.
2. В целях настоящего Положения используются следующие основные понятия:
 - 1) **персональные данные** - любая информация, относящаяся к работникам Школы или иных граждан, содержащаяся в документах, полученных Школой от субъектов персональных данных или третьих лиц.
 - 2) **оператор** – Школа; (Допускается привлекать для обработки персональных данных уполномоченные организации на основе соответствующих договоров и соглашений);
 - 3) **обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление,

хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

- 4) **распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;
- 5) **использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;
- 6) **блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
- 7) **уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;
- 8) **обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;
- 9) **информационная система персональных данных** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;
- 10) **конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;
- 11) **трансграничная передача персональных данных** - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;
- 12) **общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

13) **ИСПДн** – информационная система персональных данных.

14) **СЗПДн** – система защиты персональных данных.

ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Принципы обработки персональных данных:

- 1) законность целей и способов обработки персональных данных и добросовестности;
- 2) соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- 3) соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- 4) достоверность персональных данных, их достаточность для целей обработки, недопустимость обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- 5) недопустимость превышения сроков хранения персональных данных, объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

2. Условия обработки персональных данных.

- 2.1. В соответствии с п.2 части 2 статьи 6 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" согласие работников Школы на обработку их персональных данных не требуется.
- 2.2. Обработка персональных данных лиц, не состоящих в договорных отношениях со Школой, может осуществляться оператором только с их письменного согласия. Типовая форма такого согласия утверждается приказом директора Школы.
- 2.3. В случае, если оператор на основании договора поручит обработку персональных данных другому лицу, существенным условием такого договора должна быть обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.
- 2.4. В установленных законодательством случаях оператор обеспечивает конфиденциальность имеющихся у него персональных данных.
- 2.5. Обработка персональных данных осуществляется лицами, ответственными за обработку персональных данных, назначаемыми приказом директора Школы и производится в соответствии с «Инструкцией пользователя ИСПДн».
- 2.6. В Школе могут обрабатываться только персональные данные определенные «Перечнем персональных данных, подлежащих защите», утверждаемым приказом директора Школы.

ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ ОПЕРАТОРА ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Оператор имеет право:

- 1.1. Производить обработку персональных данных в соответствии с законодательством Российской Федерации.
- 1.2. Требовать от работников Школы и иных лиц, связанных со Школой договорными отношениями, представления персональных данных, необходимых и достаточных для исполнения предусмотренных трудовым и иным законодательством Российской Федерации функций.
- 1.3. С письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством.
- 1.4. Осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных в предусмотренных законодательством случаях.

2. Оператор обязан:

- 2.1. Производить обработку персональных данных в соответствии с соответствующим законодательством Российской Федерации и организационно-распорядительными документами Школы.
- 2.2. Принимать в соответствии с установленными требованиями необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.
- 2.3. Безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных.
- 2.4. Внести необходимые изменения, уничтожить или заблокировать соответствующие персональные данные по предоставлению субъектом персональных данных или его законным представителем сведений, подтверждающих, что его персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.
- 2.5. В случае выявления неправомерных действий с персональными данными устранить допущенные нарушения в срок, не превышающий трех рабочих дней с даты такого выявления или уничтожить персональные данные случае невозможности устранения допущенных нарушений.
- 2.6. Уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы, о внесенных изменениях или устранении допущенных нарушений либо уничтожении персональных данных

- 2.7. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных прекратить их обработку и уничтожить персональные данные в трехдневный срок и уведомить субъекта персональных данных об уничтожении персональных данных

3. Ответственность.

- 3.1. Оператор, а также работники Школы, виновные в нарушении требований законодательства о защите персональных данных, несут ответственность, предусмотренную законодательством Российской Федерации
- 3.2. Неправомерность деятельности Школы по обработке персональных данных может быть установлена в судебном порядке.

ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Субъект персональных данных имеет право:

- 1.1. Получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);
- 1.2. Осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных законодательством;
- 1.3. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства;
- 1.4. При отказе оператора или уполномоченного им лица исключить или исправить персональные данные субъекта - заявить в письменной форме о своей несогласии, представив соответствующее обоснование;
- 1.5. Дополнить персональные данные оценочного характера заявлением, выражающим его собственную точку зрения;
- 1.6. Требовать от оператора или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них;
- 1.7. Обжаловать в суд любые неправомерные действия или бездействие оператора или уполномоченного им лица при обработке и защите персональных данных субъекта.

2. Субъект персональных данных обязан:

- 2.1. Предоставлять Оператору достоверные персональные данные, а в установленных законодательством случаях – удостоверяющие персональные данные документы.
- 2.2. В установленный срок информировать Оператора об изменениях и дополнениях в составе и содержании персональных данных.
- 2.3. Информировать Оператора о ставших ему известных случаях нарушений требований защиты персональных данных.

3. Ответственность субъекта персональных данных.

Субъект персональных данных за умышленное предоставление Оператору недостоверных персональных данных несет ответственность в соответствии с законодательством.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Организационные мероприятия.

- 1.1. Для организации и координации работы по обеспечению безопасности персональных данных приказом директора Школы создается Комиссия по безопасности персональных данных (далее – Комиссия).
- 1.2. Комиссией, на основании приказа о проведении внутренней проверки, ведется периодический аудит работы Оператора по обеспечению безопасности персональных данных и на основании отчетов о результатах проведения внутренней проверки и актов классификации ИСПДн устанавливается или подтверждается класс информационной системы персональных данных, планируются и проводятся мероприятия по обеспечению безопасности персональных данных.
- 1.3. Комиссией разрабатываются проекты организационно-распорядительных документов, регламентирующих работу Оператора по обеспечению безопасности персональных данных.
- 1.4. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе приказом директора Школы назначается должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.
- 1.5. Работники, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании приказа о назначении ответственных лиц за обработку ПДн.
- 1.6. Комиссия:
 - определяет угрозы безопасности персональных данных при их обработке и формирует на их основе модели угроз;
 - разрабатывает 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;
 - организует обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
 - проводит 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;

2. Технические мероприятия.

- 2.1. Организация и ведение работы по техническому обеспечению и сопровождению работы по защите персональных данных, созданию и поддержанию в нормативном состоянии системы защиты персональных данных приказом директора Школы возлагается на администратора безопасности ИСПДн.
- 2.2. Администратор безопасности ИСПДн определяет и устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в соответствии с законодательством Российской Федерации и нормативно-методическими актами уполномоченных регулирующих органов. Выбранные и реализованные методы и способы защиты информации должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах в составе создаваемой Оператором системы защиты персональных данных.
- 2.3. Администратор безопасности ИСПДн обеспечивает:
 - 1) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
 - 2) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
 - 3) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
 - 4) контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
 - 5) своевременное обнаружение фактов несанкционированного доступа к персональным данным;
 - 6) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
 - 7) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.