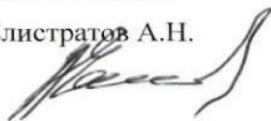


ПРИНЯТО
на заседании
коллективного собрания
протокол от 27.05.2015
№ 9

СОГЛАСОВАНО
Председатель
Совета школы
Елистратов А.Н.



УТВЕРЖДЕНО
Приказом по МБОУ СОШ №1
от 27.05.2015 № 46-1
Директор Б.Н.Воробьев



Положение
о порядке обеспечения конфиденциальности при обращении
с информацией, содержащей персональные данные,
в МБОУ СОШ № 1

1. Общие положения

1.1 Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные, в МБОУ СОШ № 1 обязательна для всех структурных подразделений ОУ, устанавливает требования по обеспечению конфиденциальности документов, содержащих персональные данные, и разработана на основании Трудового кодекса Российской Федерации, Федерального закона от 27.06.2006 № 152-ФЗ "О персональных данных", постановлений Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

1.2 Персональными данными является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, социальное, имущественное положение, образование, профессия, доходы, другая информация.

1.3 Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных или в отношении общедоступных персональных данных, в том числе справочники, адресные книги, в которые в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

1.4 Конфиденциальность персональных данных предусматривает обязательное согласие субъекта персональных данных или наличие иного законного основания на их обработку.

1.5 Согласие субъекта персональных данных не требуется на обработку персональных данных:
– в целях исполнения обращения, запроса субъекта персональных данных, трудового или иного договора с ним;

– адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;

– данных, включающих в себя только фамилии, имена и отчества;

– в целях однократного пропуски на территорию или в иных аналогичных целях;

– персональных данных, обрабатываемых без использования средств автоматизации.

1.6 В структурных подразделениях МБОУ СОШ № 1 формируется и ведется перечень конфиденциальных данных с указанием регламентирующих документов, мест хранения и ответственных за хранение и обработку данных. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.

2. Основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных в информационных системах

2.1 Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

2.2 Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

2.3 Информационные системы классифицируются ОУ, осуществляющей обработку персональных данных, а также определяющей цели и содержание обработки персональных данных, в зависимости от

объема обрабатываемых персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства в порядке, предусмотренном приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 N 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».

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

2.5 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.

2.6 Безопасность персональных данных при их обработке в информационной системе обеспечивают должностные лица ОУ, определенные приказом директора школы.

2.7 При обработке персональных данных в информационной системе должно быть обеспечено:

- а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- д) постоянный контроль за обеспечением уровня защищенности персональных данных.

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

- а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- б) 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;
- в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- ж) учет лиц, допущенных к работе с персональными данными в информационной системе;
- з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- и) 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;
- к) описание системы защиты персональных данных.

2.8 Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе в МБОУ СОШ № 1 приказом директора назначается должностное лицо (работник), ответственный за обеспечение безопасности персональных данных.

2.9 Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного приказом директора.

2.10 Запросы пользователей информационной системы на получение персональных данных, допущенных к персональным данным лиц, а также факты предоставления персональных данных по

этим запросам регистрируются журнале обращений. Содержание журнала обращений периодически проверяется соответствующими должностными лицами (работниками) ОУ.

2.11 При обнаружении нарушений порядка предоставления персональных данных предоставление персональных данных пользователям информационной систем незамедлительно приостанавливается приказом директора школы до выявления причин нарушений и устранения этих причин.

2.12 Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

3. Основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных без использования средств автоматизации

3.1 Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

3.2 При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

3.3 Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы руководителем о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами ОУ.

3.4 При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес ОУ, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых учреждением способов обработки персональных данных; б) типовая форма должна предусматривать поле, в котором субъект персональных данных может

поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных; в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных

данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных; г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных

данных, цели обработки которых заведомо не совместимы.

3.5 При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных; б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих

уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

3.6 Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.7 Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3.8 Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

3.9 Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.10 При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются приказом директора школы.

4. Должностные обязанности лиц, обрабатывающих персональные данные и допущенных к ним

4.1 Все сотрудники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных.

4.2 Запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении.

4.3 Сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не связано со служебной необходимостью.

4.4. Без согласования с лицом, ответственным за защиту персональных данных в ОУ, формирование и хранение баз данных (карточек, файловых архивов и др.), содержащих конфиденциальные данные запрещается.

4.5 Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан.

4.6 Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

5. Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и утилизации

5.1 Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учету. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер. Учет и выдачу съемных носителей персональных данных осуществляют сотрудники, на которых возложены функции хранения носителей персональных данных. Сотрудники ОУ получают учетный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнал учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

5.2. Запрещается:

- хранить съемные носители с персональными данными вместе с носителями открытой информации на рабочих столах либо оставлять их без присмотра или представлять на хранение другим лицам; - выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому и т. д.

5.3. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных

носителях осуществляется в порядке, установленном для документов служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя..

5.4. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель учреждения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журнал учета съемных носителей персональных данных. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется соответствующий акт.

6. Ответственность

6.1 Сотрудники, осуществляющие обработку или хранение конфиденциальных данных в академии, несут ответственность за обеспечение их сохранности и безопасности.

6.2 Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами.