

Муниципальное бюджетное общеобразовательное учреждение
«Школа № 89»
городского округа Самара

ПРИНЯТО:

«01» февраля 20 16 г.

Протокол Совета школы № _____

Председатель Оксисекал

УТВЕРЖДАЮ: т.р. и Бог

«01» февраля 20 16 г.

Директор МБОУ «Школа № 89»

г.о. Самара

И.Ф. Новосельцева

Положение о защите персональных данных работников
муниципального бюджетного общеобразовательного учреждения
«Школа № 89» г.о. Самара

Самара.2016

1. Общие положения

Настоящее положение о защите персональных данных устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным сотрудников и учеников МБОУ «Школа № 89» г.о. Самара.

2. Цель

Настоящее положение о защите персональных данных является развитием комплекса мер, направленных на обеспечение защиты персональных данных, посредством планомерных действий по совершенствованию организации труда.

3. Понятие и состав персональных данных

Под персональными данными сотрудников и учащихся понимается информация, необходимая в связи с трудовыми отношениями и обучением, касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника или учащегося, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

К персональным данным относятся:

- все биографические сведения ;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора или личного дела;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т2) и трудовые книжки сотрудников;

- основания к приказам;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников; их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкета;
- копии документов об образовании и личные дела;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии;
- и т.п.

Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом. Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Субъект (законный представитель) персональных данных самостоятельно решает вопрос передачи работодателю своих персональных данных.

Держателем персональных данных является МБОУ «Школа № 89», которому сотрудники , ученики и родители (законные представители) добровольно передают во владение свои персональные данные и который выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

Права и обязанности работодателя в трудовых отношениях с сотрудниками осуществляются физическим лицом, уполномоченным работодателем, в отношениях с учащимися указанными правами и обязанностями обладают назначенные руководителем классные руководители.

Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

4. Доступ к персональным данным

Персональные данные добровольно передаются сотрудником непосредственно держателю этих данных и потребителям внутри МБОУ «Школа № 89» исключительно для обработки и использования в работе.

1). Внешний доступ. К числу массовых потребителей персональных данных можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

2). Внутренний доступ. Внутри МБОУ ООШ № 89 к разряду потребителей персональных данных относятся сотрудники, которым эти данные необходимы для выполнения должностных обязанностей.

В кадровом секторе хранятся личные карточки сотрудников, работающих в настоящее время и личные дела обучающихся, обучающихся в настоящее время. Для этого используется сейф и кабинет директора школы, которые запираются, ключи от кабинета и сейфа находятся у директора и заместителя директора по УВР. После увольнения документы по личному составу отправляются в архив на хранение, личные дела выдаются родителям по заявлению.

Личные данные хранятся в электронном виде в бухгалтерии, доступ к компьютеру имеет пароль.

5. Передача персональных данных

При передаче персональных данных сотрудника или ученика держатель должен соблюдать следующие требования:

1). Передача внешнему потребителю.

- Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только

в целях выполнения задач, соответствующих объективной причине сбора этих данных.

- При передаче персональных данных потребителям держатель не должен сообщать эти данные третьей стороне без письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью.

- Ответы на правомерные письменные запросы учреждений и организаций даются с разрешения директора и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений.

- Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

- Сведения передаются в письменной форме и должны передаваться лично.

- По возможности персональные данные обезличиваются.

2). Передача внутреннему потребителю.

- Внутренние потребители персональных данных берут на себя обязательство о неразглашении персональных данных сотрудников.

6. Защита персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

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.

Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе образовательной деятельности школы.

1). «Внутренняя защита».

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и

базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и сотрудниками.

Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
- знание сотрудниками требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и электронными данными;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- своевременное выявление нарушения требований разрешительной системы доступа к персональным данным;
- воспитательная и разъяснительная работа с сотрудниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел учеников посторонним лицам и за пределы кабинета директора. Личные дела могут выдаваться классным руководителям в исключительных случаях лично директором школы;
- персональные компьютеры, на которых содержатся персональные данные, должны быть защищены паролями доступа.

2). «Внешняя защита».

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, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения, посетители, сотрудники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов .

Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- пропускной режим ;
- порядок охраны территории, здания, помещений, транспортного средства;
- требования к защите информации при интервьюировании и собеседованиях.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными.

Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

Каждый сотрудник , получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско–правовую или уголовную ответственность граждан и юридических лиц.