Приложение № 9
к коллективному договору

Первичная профсоюзная организация
МБОУ Школа № 29
г.о. Самара
Председатель ПК _____М.Н. Цветкова
«28» 08 2019 г.

Директор МБОУ Школа № 29 г.о. Самара
_____ И. М. Атапина
«28» 08 2019 г.

ПОЛОЖЕНИЕ
о защите персональных данных муниципального бюджетного общеобразовательного учреждения «Школа № 29 имени начальника Управления пожарной охраны УВД Самарской области Карпова А.К.» городского округа Самара

1. Общие положения.

1.1 Настоящее положение принято в целях сохранения личной тайны и защиты персональных данных работников МБОУ Школа № 29 г. о. Самара.
1.2 Положение определяет права и обязанности руководителей, работников, порядок использования указанных данных в служебных целях, а также порядок взаимодействия по поводу сбора, документирования, хранения и уничтожения персональных данных.
1.3 Настоящее Положение разработано на основании:
-статей Конституции РФ; Трудового Кодекса РФ глава 14 «О защите персональных данных работника»;
-Федерального закона № 152 «О персональных данных»;
-Письма Рособробразования от 29.07.2009 № 17-110 «Об обеспечении защиты персональных данных»;
- Приказа № 1\23от 01.09.2011 о приведении документооборота в соответствии с ФЗ «О персональных данных»;
-Постановления Правительства РФ от 01.11.2012 № 1119 «Требования к защите персональных данных при их обработке»
1.4 Локальные нормативные акты школы о персональных данных должны быть доступны на сайте школы school29@.bk.ru и в печатном виде (в канцелярии).

2. Понятие и состав персональных данных работников

2.1 Основные термины, используемые в настоящем Положении:
2.1.1 Персональные данные (далее ПДн) - 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, контактные телефоны, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
2.1.2 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;

2.1.3 Распространение персональных данных – действия, направленные на передачу 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-коммуникативных сетях или предоставление доступа к персональным данным каким-либо иным способом.

2.1.4 Использование персональных данных - действия (операции) с персональными данными, совершаемые 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;

2.1.5 Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

2.1.6 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;

2.1.7 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 (далее информационная система);

2.1.8 Технические средства, позволяющие осуществлять обработку персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео - и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

2.2. Персональные данные работника составляют:

- сведения о фактах, событиях и обстоятельствах частной жизни работника, позволяющие идентифицировать его, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- служебные расследования, а также иные сведения, связанные с профессиональной деятельностью работника, в том числе сведения о поощрениях и о дисциплинарных взысканиях.

2.2.1 Документами, содержащие персональные данные являются:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о постановке на учёт в налоговый орган и присвоения ИНН;
- документы воинского учёта;
- документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки;
- карточка Т-2;
- автобиография;

- личный листок по учёту кадров;
- медицинское заключение о состоянии здоровья;
- документы, содержащие сведения о заработной плате, доплатах и надбавках, стимулирующих баллах;
- приказы о приеме лица на работу, об увольнении, а также о переводе лица на другую должность;
- другие документы, содержащие сведения, предназначенные для использования в служебных целях.

2.3.Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения, соответствующий гриф ограничения на них не ставится. Режим конфиденциальности ПДн снимается в случаях обезличивания или по истечении 75- летнего срока хранения, если иное не определено законом.

3. Порядок получения, обработки и хранения персональных данных

3.1. Под обработкой ПДн понимается получение, хранение, комбинирование, передача или другое использование персональных данных Документы, содержащие персональные данные, создаются путём:

а) копирования оригиналов документов;

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

3.2. В целях обеспечении прав и свобод человека и гражданина школа и ее представители при обработке ПДн обязаны соблюдать следующие общие требования:

3.2.1. Обработка ПДн может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, регламентирующих образовательную деятельность учреждения;

3.2.2. При определении объема и содержания, обрабатываемых ПДн школа руководствуется Конституцией РФ, нормативными и распорядительными документами Минобрнауки России, Минобрнауки Самарской области, Рособразования, Рособрнадзора и Устава школы;

3.2.3. Работники и их представители должны быть ознакомлены под расписку с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.2.4. Школа не имеет права получать и обрабатывать ПДн о политических, религиозных и иных убеждениях и частной жизни субъектов персональных данных.

3.2.5. Школа не имеет права получать и обрабатывать ПДн о членстве в общественных объединениях или профсоюзной деятельности субъектов персональных данных, за исключением случаев, предусмотренных федеральным законом;

3.3. Сведения, содержащие персональные данные работника, включаются в его личное дело, карточку формы Т-2, а также содержатся на электронных носителях информации, доступ к которым разрешён лицам, непосредственно использующих персональные данные работника в служебных целях. К обработке, передаче и хранению ПДн могут иметь доступ сотрудники, список которых утвержден приказом директора школы. Список должностей, имеющих доступ к персональным данным, представлен в Приложении №1.

3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан РФ. Ограничение прав граждан РФ на основе использования информации об их социальном происхождении, их расовой, национальной, языковой, религиозной, партийной принадлежности запрещено и карается в соответствии с законодательством.

3.9. Все меры обеспечения безопасности при сборе, обработке и хранении Пдн распространяются как на бумажные, так и на электронные (автоматизированные) носители

информации.
3.10. Все меры конфиденциальности при сборе, обработке и хранении ПДн сотрудников распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.
3.11. Персональные данные, включённые в состав личных дел, хранятся в запираемом шкафу, установленном на рабочем месте специалиста по кадрам. Персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК специалиста по кадрам.
3.12. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу, только по официальному запросу. Предоставление ПДн государственным органам производится в соответствии с требованиями действующего законодательства и настоящим Положением.
3.13. Персональные данные, включённые в состав личных дел, хранятся в запираемом шкафу, установленном на рабочем месте специалиста по кадрам. Персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК специалиста по кадрам.
3.14. Трудовая книжка, документы воинского учёта, карточка формы Т-2 хранятся в запертом металлическом сейфе.
Доступ к ПК строго ограничен кругом лиц, определённых в пункте 4.1. настоящего Положения. Персональные данные, содержащиеся на бумажных носителях, сдаются в архив после истечения установленного срока хранения.

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри организации) имеют:

- Директор школы;
- Главный бухгалтер
- Секретарь школы
- Специалист по кадрам;
- Заместитель по технике безопасности;
- Методист АСУ РСО;

4.2. Внешний доступ:
4.2.1 к числу массовых потребителей персональных данных вне организации можно отнести государственные, функциональные структуры: налоговые инспекции, правоохранительные органы, органы статистики, военкоматы, органы социального страхования, пенсионные фонды, подразделения муниципальных органов управления;
4.2.2 надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции;
4.2.3 другие организации: Министерство образования и науки Самарской области, Департамент образования городского округа Самара, региональные и городские комитеты проводимых конкурсов.

5. Защита персональных данных

5.1. Защита прав, установленных настоящим Положением и законодательством РФ, осуществляется судом, в целях пресечения неправомерного использования персональных данных, восстановления нарушенных прав и возмещения ущерба, в том числе морального вреда.
5.2. Лица, виновные в нарушении норм, регулирующие получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или головную ответственность в соответствии с федеральными законами.
5.3. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена школой за счет ее средств, в порядке, установленном федеральным законом.

5.4. ОУ обязано обеспечить безопасность персональных данных при их обработке в информационной системе. Защита персональных данных содержится на электронных носителях или в программно-технических средствах, обеспечивающее исключение доступа к ресурсам сети Интернет.
5.5. Все сотрудники имеющие доступ к хранению ПДн, обязаны подписать соглашение об их неразглашении. Руководитель, разрешающий доступ сотрудника к документу с ПДН, несет персональную ответственность за данное разрешение.
5.6. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.
5.7. 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.

6. Права и обязанности работников

6.1. В целях обеспечения защиты персональных данных, хранящихся в личных делах, работники имеют право:

- получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);
- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные за исключением случаев, предусмотренных федеральным законом;
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением федерального закона. Работник, при отказе работодателя исключить или исправить персональные данные имеет право заявлять в письменной форме работодателю о своём несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требовать от работодателя уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведённых в них изменениях или исключениях из них;
- обжаловать в суд любые неправомерные действия или бездействие работодателя при обработке и защите персональных данных.
- Запрещается передавать информацию о состоянии здоровья работника за исключением сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

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

7.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.
7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством РФ за нарушение режима защиты, обработки и порядка использования этой информации.
7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.
7.4. Каждый сотрудник школы, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность

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

7.5. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания. К данным лицам могут быть применены следующие дисциплинарные взыскания:

- замечание;
- выговор;
- предупреждение о неполном должностном соответствии;
- освобождение от занимаемой должности;
- увольнение по соответствующим основаниям.

7.6. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

7.7. Копия приказа о применении к работнику дисциплинарного взыскания с указанием оснований его применения вручается работнику под роспись в течение трех рабочих дней со дня издания приказа не считая времени отсутствия работника на работе. Если работник отказывается ознакомиться с приказом под роспись, то составляется соответствующий акт.

7.8. Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Работодатель до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с работника по собственной инициативе, по письменному заявлению работника или по ходатайству его непосредственного руководителя.

7.9. Должностные лица, в обязанность которых входит ведение персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных нарушениях.

7.9.1. В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющие служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

7.9.2. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собрание или распространение сведений о частной жизни лица, составляющую его личную или семейную тайну, без его согласия) неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, арестом в соответствии с УК РФ.

7.10. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть использована в судебном порядке.

Приложение №1

Список должностей,
имеющих доступ к персональным данным работников школы

- Директор школы;
- Секретарь школы,
- Специалист по кадрам;
- Главный бухгалтер;
- Заместитель по технике безопасности;
- Методист АСУ РСО.

.