

согласия работника, если иное не предусмотрено законодательством.

1.9. Работодатель имеет право собирать персональную информацию, содержащуюся в документах, предоставленных работником при приеме на работу.

1.10. Работодатель производит расчет и выплату налогов за работника путем удержания их из заработной платы, работодатель имеет право собирать предусмотренные Налоговым Кодексом РФ сведения о налогоплательщике.

1.11. Данное Положение предотвращает несанкционированный доступ к информации, ее противоправное копирование, искажение, использование преднамеренного распространения недостоверной информации, использование информации в преступных и корыстных целях.

**II. Порядок хранения, использования и передачи персональных данных работника**

Хранение персональных данных должно исключать их утрату или их неправильное использование. 2.1.Хранение, выдача трудовых книжек (дубликаты трудовых книжек); хранение личных дел

работников и иных документов, отражающих персональные данные работника, возлагаются на руководителя, делопроизводителя и работников бухгалтерии (список лиц утверждается приказом по школе).

2.2.Персональные данные работников вместе с необходимыми документами остаются у работодателя или лица, ответственного за оформление приема и хранения личных дел сотрудников. Порядок хранения трудовых книжек установлен Инструкцией по заполнению трудовых книжек.

2.2.1. Работодатель обеспечивает хранение первичных документов, связанных с обработкой документации по учету труда, кадров и оплаты труда в организации. В бухгалтерии хранятся документы по учету использования рабочего времени и расчетов с персоналом по оплате труда.

2.2.2. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

|  |  |  |
| --- | --- | --- |
| 2.2.2.1. | Не сообщать персональные данные работника третьей стороне без | письменного |
| согласия | работника, за исключением случаев, когда это необходимо в целях предупреждения |
| угрозы жизни и здоровью работника, а также в случаях, установленных Федеральным законом; |
| 2.2.2.2. | Не сообщать персональные данные работника в коммерческих целях без его |
| письменного согласия. |  |
| 2.2.2.3. | Предупредить лиц, получающих персональные данные работника, о | том, что эти |

данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном Федеральными законами.

2.2.2.4. Разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций.

2.2.2.5. Передавать персональные данные работника представителям работников в порядке, установленном ТК РФ, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

2.2.2.6. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции; передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

2.2.3. Передача персональных данных работника в пределах организации:

2.2.3.1. Работодатель предоставляет информацию и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов, обязательных платежей в государственную бюджетную систему: документы о платежеспособности, сведения о численности, составе

работающих, заработной плате и условиях труда, о наличии свободных рабочих мест; документы об оплате налогов по требованию органов власти управления, правоохранительных органов, юридических лиц, имеющих на это право.

2.2.3.2. Предоставляемая информация может быть устной или письменной, во втором случае

– заверена печатью и подписями определенных лиц.

1. **Обязанности работодателя по хранению и защите персональных данных работника**

3.1. Работодатель обеспечивает защиту персональных данных работника от неправомерного их использования или утраты за счет собственных средств, в порядке, установленном федеральным законом.

3.2.Работодатель знакомит работника под роспись со всеми внутренними документами, касающимися порядка обработки, передачи персональных данных работников, о правах и обязанностях в этой области.

3.3.Работодатель обеспечивает доступ к персональным данным работника только уполномоченным лицам.

3.4.Руководитель закрепляет в Приказе по ОО распределение обязанностей по обработке персональных данных.

3.5.Запрещается обработка информации в присутствии иных лиц, кроме имеющих право доступа к персональным данным работника. Руководитель хранит документы (трудовые книжки в сейфе); рекомендуется при обработке данных с помощью компьютера закрывать паролем файлы, имеющие персональные данные.

**IV. Права работников на защиту персональных данных**

4.1.Согласно ст.89 Трудового Кодекса РФ работники имеют право на:

4.2.Полную информацию об их персональных данных и обработке этих данных.

4.3.Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных Федеральным законом.

4.4.Определение своих представителей для защиты своих персональных данных.

4.5.Доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору.

4.6.Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения.

4.7.Требование об извещении работодателем всех лиц, которым раннее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

4.8.Работники должны быть ознакомлены под роспись с настоящим Положением. С этой целью в учреждении организуется и ведется Журнал ознакомления работников с настоящим Положением.

4.9.Обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

**V. Ответственность работодателя и лиц, осуществляющих работу с персональными данными**

5.1. Работник обязан:

* знать Перечень сведений конфиденциального характера в школе;
* хранить в тайне известные ему конфиденциальные сведения, информировать руководителя о фактах нарушения порядка обращения с конфиденциальными сведениями, о ставших ему

известным попытках несанкционированного доступа к информации;

* соблюдать правила пользования документами, порядок их учета и хранения, обеспечивать в процессе работы сохранность информации, содержащейся в них от посторонних лиц;
* знакомиться только с теми служебными документами, к которым получен доступ в силу исполнения своих служебных обязанностей.

5.2.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.

5.3.К сотруднику, ответственному за хранение персональной информации работников, работодатель вправе применить одно из дисциплинарных взысканий, предусмотренных ст. 192 ТК РФ, а именно: замечание, выговор, увольнение. К дисциплинарной ответственности привлекаются только те работники, которые по условиям своих трудовых договоров обязаны соблюдать правила работы с персональными данными.

5.4.Работодатель вправе расторгнуть трудовой договор по своей инициативе при разглашении охраняемой законом тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей.

Приложение № 1

**ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПОДЛЕЖАЩИХ ЗАЩИТЕ И ОБРАБАТЫВАЕМЫХ В ШКОЛЕ**

**I. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Перечень персональных данных, подлежащих обработке и защите (далее – Перечень), разработан в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152 «О персональных данных».

1.2. Перечень содержит полный список категорий данных, безопасность которых должна обеспечиваться системой защиты персональных данных (СЗПДн).

**II. СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ**

2.1. Персональные данные работников:

* фамилия, имя, отчество (в том числе прежние);
* место, год и дата рождения;
* адрес по прописке;
* адрес проживания (реальный);
* паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство;
* информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающих образование: наименование, номер, дата выдачи, специальность);
* информация о трудовой деятельности до приема на работу;
* информация о трудовом стаже (место работы, должность, период работы, причины увольнения);
* телефонный номер (домашний, рабочий, мобильный);
* семейное положение и состав семьи (муж/жена, дети);
* информация о знании иностранных языков;
* оклад;
* сведения об оплате труда;
* сведения о начисляемых и удерживаемых страховых взносах из заработной платы;
* номера счетов для расчета с работниками;
* данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменений к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
* сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
* ИНН;

-сведения о номере и серии страхового свидетельства государственного пенсионного страхования;

* информация о наличии судимости;
* данные об аттестации работников;
* данные о повышении квалификации;
* данные о наградах, медалях, поощрениях, почетных званиях;
* информация о периодах нетрудоспособности;
* информация о болезнях;
* информация о командировках;
* сведения, указанные в оригиналах и копиях приказов по личному составу школы и материалах к ним;
* материалы по внутренним служебным расследованиям в отношении работников школы.

2.2.Персональные данные субъектов ПДН (учащихся):

* фамилия, имя, отчество;
* дата и место рождения;
* паспортные данные;
* контактный телефон;
* адрес прописки;
* адрес фактического проживания;
* данные о социальных и жилищных условиях;
* данные о материальном положении учащихся;
* данные о наградах и достижениях учащихся;
* данные о состоянии здоровья учащихся.

 Приложение № 2

**ИНСТРУКЦИЯ**

**пользователя по обеспечению информационной безопасности автоматизированного**

**рабочего места, выделенного для обработки конфиденциальной информации**

**(персональных данных)**

Настоящий документ разработан на основе Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 г. №

* 1. Инструкции пользователя по обеспечению информационной безопасности при работе с базами данных школы (далее – Инструкция пользователя) использованы следующие термины и определения:
1. База данных (далее - БД) - централизованное хранилище информации, оптимизированное для многопользовательского доступа и работающее под управлением системы управления базами данных (далее - СУБД).
2. Комплекс программных средств (далее - КПС) - система или приложение, использующее непосредственный доступ к БД.
3. Идентификатор (учетное имя или login) - присвоенная пользователю индивидуально буквенно-числовая последовательность, используемая для идентификации пользователя при установлении доступа к БД и позволяющая однозначно определять работу конкретного пользователя в БД.
4. Пароль - секретная персональная последовательность символов, известная только пользователю, которая используется совместно с идентификатором для доступа в БД и позволяет подтвердить, что доступ к БД осуществляет именно конкретный пользователь.
5. Пользователи - должностные лица школы, а также все другие лица и организации, работающие с БД школы.
6. Администратор БД - должностное лицо школы, уполномоченное для выполнения административных функций и обеспечивающие функционирование БД и ее безопасность соответственно.
7. Локально-вычислительная сеть (далее - ЛВС) - группа компьютеров, а также периферийное оборудование, объединенные одним или несколькими автономными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.
8. Политика информационной безопасности - комплекс организационно-технических мероприятий, правил и условий использования информационных систем школы, определяющих нормальное функционирование систем и обеспечение безопасности информации, обрабатываемой в школе.

**Обязанности и ответственность**

1. Перед началом первой работы с конфиденциальной информацией пользователь обязан изучить Инструкцию пользователя и ознакомиться с ответственностью за выполнение требований Инструкции пользователя при работе с конфиденциальной информацией под роспись.
2. Пользователю запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа к конфиденциальной информации другим лицам. Запрещается хранение пароля в общедоступных местах, позволяющих другим лицам получить информацию о пароле.
3. Пользователь конфиденциальной информации обязан обеспечивать правильность ввода и коррекции данных, за которые он отвечает.
4. Пользователь обязан закрывать соединение с БД школы на время своего отсутствия у рабочей станции БД или вообще выходить по доступу к ресурсам компьютера с конфидициальными данными из своего идентификатора (например, teacher, secret, adminic и т.п., через Пуск - Завершить сеанс - Имя идентификатора).
5. В случае выявления инцидентов с доступом к ресурсам компьютера с конфиденциальными данными (фактов несанкционированного доступа посторонними людьми, людьми без допуска к конфиденциальным данным) пользователь обязан незамедлительно сообщить об этом системному

администратору школы.

1. В случае выявления инцидентов с доступом к БД школы (фактов несанкционированного доступа к БД, блокировки доступа, утери или компрометации пароля и т.п.) пользователь обязан незамедлительно сообщить об этом администратору БД.
2. Установку и конфигурирование программного обеспечения на компьютерах с доступом к конфиденциальным данным школы выполняет системный администратор или администратор БД школы. Пользователям данных рабочих мест запрещается самостоятельно устанавливать какое-либо программное обеспечение.
3. Пользователю запрещается использовать информацию, полученную в результате доступа к конфиденциальным данным школы, в целях, не предусмотренных его функциональными обязанностями и технологическими схемами. Он не вправе разглашать, использовать в личных целях, либо передавать третьим лицам, в том числе государственным органам, конфиденциальную информацию, за исключением случаев, установленных законами Российской Федерации.
4. При нарушениях правил, связанных с информационной безопасностью, пользователь несет ответственность, установленную действующим законодательством Российской Федерации.
5. Пользователь несет ответственность за все действия, совершенные от имени его идентификатора, учетной записи или логина, если не доказан факт несанкционированного использования таковых.