

**МУНИЦИПАЛЬНОЕ КАЗЁННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ВОРОБЬЁВСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА ИМЕНИ
ГЕРОЯ СОВЕТСКОГО СОЮЗА НИКОЛАЯ ТИМОФЕЕВИЧА ВОРОБЬЁВА»
(МКОУ «Воробьёвская СОШ имени Н.Т.Воробьёва»)**

ИНН 0807003088 ОГРН 1020800671264

Республика Калмыкия. Приютненский район, с. Воробьёвка, ул. Мира, д. 51
email: irjkfdci@yandex.ru



Приказ №__ от «__»__ 20__ г.

Принято на заседании
педагогического совета

Протокол №__ от «__»__ 20__ г.

ПОЛОЖЕНИЕ

защите персональных данных работников

МКОУ «Воробьёвская СОШ имени Н.Т.Воробьёва»

с.Воробьёвка, 20__ год.

1. Общие положения

1.1. Настоящее Положение о защите персональных данных работников (далее Положение) муниципального казённого общеобразовательного учреждения средней общеобразовательной школы имени Героя Советского Союза Николая Тимофеевича Воробьёва» (далее МКОУ «Воробьёвская СОШ им. Н.Т.Воробьёва»), разработано на основании статей Конституции РФ, Трудового кодекса РФ, Кодекса РФ об административных правонарушениях, Гражданского кодекса РФ, Уголовного кодекса РФ, а также Федерального закона "Об информации, информатизации и защите информации" и «О персональных данных».

1.2. Целью данного Положения является определение порядка обработки персональных данных работников МКОУ «Воробьёвская СОШ им. Н.Т.Воробьёва»; обеспечение защиты прав и свобод работников при обработке их персональных данных, от несанкционированного доступа, неправомерного их использования или утраты, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников и обучающихся.

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.4. Настоящее Положение утверждается и вводится в действие приказом руководителя образовательного учреждения и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

2. Основные понятия и состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

- персональные данные – информация (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация), необходимая руководителю в связи с трудовыми отношениями и касающиеся конкретного работника или для ведения образовательного процесса;

- обработка персональных данных — сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;

- конфиденциальность персональных данных — обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия работника или иного законного основания;

- 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 работников каким-либо иным способом;

- использование персональных данных — действия (операции) с персональными данными, совершаемые должностным лицом МКОУ «Воробьёвская СОШ им. Н.Т.Воробьёва» в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников или обучающихся либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

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

- 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;

- обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному лицу;

- общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или родителя (законного представителя); или персональные данные, на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

- документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2. В состав персональных данных входят:

- анкетные и биографические данные;
- образование;
- документ об образовании, о квалификации или наличии специальных знаний — при поступлении на работу, требующую специальных знаний или специальной подготовки;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о присвоении ИНН;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела сотрудников и обучающихся;
- трудовые книжки;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики.

2.3. Документы, указанные в п. 2.2. настоящего Положения, являются конфиденциальными.

3.2.2. При определении объема и содержания обрабатываемых персональных данных руководитель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными федеральными законами.

3.2.3. Персональные данные следует получать у работников. Если персональные данные возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие (*Приложение № 1*). Руководитель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.2.4. Руководитель не имеет права получать и обрабатывать персональные данные о политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны руководителем только с его письменного согласия.

Обработка указанных персональных данных работников руководителем возможна только с их согласия либо без их согласия в следующих случаях: – персональные данные являются общедоступными; персональные данные относятся к состоянию здоровья и их обработка необходима для защиты их жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;

– по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

3.2.5. Руководитель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.2.6. Руководитель вправе обрабатывать персональные данные только с письменного согласия работника (*Приложение № 2*).

3.3. Порядок обработки, передачи и хранения персональных данных.

3.3.1. Работник предоставляет директору Учреждения достоверные сведения о себе. Директор проверяет достоверность сведений, сверяя предоставленные данные, с имеющимися документами.

3.3.2. В целях обеспечения прав и свобод человека и гражданина руководитель и его представители при обработке персональных данных должны соблюдать законы и иные нормативные правовые акты.

4. Передача и хранение персональных данных.

4.1. Передача персональных данных возможна только с согласия работника, или в случаях, прямо предусмотренных законодательством.

4.2. При передаче персональных данных должны соблюдаться следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника (*Приложение № 3*), за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- 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;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по Учреждению, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

4.3. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

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

4.5. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

5. Доступ к персональным данным.

5.1. Внутренний доступ (доступ внутри организации).

5.1.1. Право доступа к персональным данным сотрудника имеют:

- директор;
- заместители директора;
- сам работник, носитель данных;
- другие сотрудники при выполнении ими своих служебных обязанностей.

5.2. Внешний доступ.

5.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

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

5.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

5.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

5.2.3. Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника. В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия (УК РФ).

6. Защита персональных данных.

6.1. 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.

6.2. 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.

6.3. 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 управленческой деятельности школы.

6.4. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена руководителем за счет его средств в порядке, установленном федеральными законами.

6.5. Внутренняя защита.

6.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

6.5.2. Для обеспечения внутренней защиты персональных данных необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;

- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации;
- воспитательная и разъяснительная работа с сотрудниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

6.5.3. Защита персональных данных на электронных носителях.

Все папки, содержащие персональные данные, должны быть защищены паролем.

6.6 Внешняя защита.

6.6.1. 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.

6.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности школы. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов.

6.6.3. Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим Учреждения;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств.

6.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников (*Приложение № 4*).

6.8. По возможности персональные данные обезличиваются.

7. Права и обязанности работника.

7.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

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

7.3. В целях защиты персональных данных, хранящихся у руководителя, работник имеет право:

- требовать исключения или исправления неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны;

- отозвать согласие на обработку персональных данных (*Приложение № 5*).

7.4. Работник обязан:

- передавать руководителю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;
- своевременно сообщать руководителю об изменении своих персональных данных.

7.5. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

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

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

8.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

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

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

8.5. 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.

8.5.1. 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.

8.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, 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 правонарушениях.

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

8.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего 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 наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

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

Правительство Российской Федерации на основании конституционных принципов защиты личности и свободы информации

Д. _____ 2014 года

С целью, предусмотренной в законе, и с целью обеспечения персональной защиты, и защиты и документирования данных, полученных в результате деятельности и взаимодействия между собой, и взаимодействия с другими субъектами.

1. Защита личности может осуществляться только с помощью личности, осуществляющей личную работу.
2. Необходимость защиты личности, обеспечивающей и обеспечивающей взаимодействие, и обеспечивающей защиту личности от других лиц.
3. Защита личности, обеспечивающей личность, обеспечивающую личность, обеспечивающую личность.

Приложение 1

МКОУ «Воробьевская им.
Н.Т.Воробьева» Л.П
Фоменко Е.В.

_____ (ФИО, должность работника)

_____ (дата рождения)

проживающий по адресу: _____

паспорт:
выдан: _____

Письменное согласие работника на получение его персональных данных у третьей стороны

Я, _____, в соответствии со ст. 86 ТК РФ
на получение моих персональных данных, _____

(согласен, не согласен)

а именно:

(Ф.И.О. физического лица или наименование организации, у которых получается информация)

О целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение предупрежден.

"__" _____ 20__ г. _____

Подпись _____ ФИО работника

Примечание:

1. Вместо паспорта могут указываться данные иного основного документа, удостоверяющего личность работника.
2. Письменное согласие работника заполняется и подписывается им собственноручно, в присутствии сотрудника отдела кадров.
3. Перечень персональных данных уточняется исходя из целей получения согласия.

ПИСЬМЕННОЕ СОГЛАСИЕ

на обработку персональных данных работника

Я, _____

Проживающий по адресу _____

Паспорт серия _____ номер _____ выдан _____

в соответствии со статьей 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» даю в МКОУ «Воробьевская СОШ им. Н.Т.Воробьева» согласие на обработку моих следующих персональных данных: о фамилии, имени, отчестве, дате и месте рождения, месте регистрации и проживания, контактных телефонах, семейном положении, ближайших родственниках; о паспортных данных, номере ИНН, страхового пенсионного свидетельства, медицинского полиса; об образовании (оконченное учебное заведение и год окончания, специальность и (направление) и квалификация, наличие ученых званий (степеней), даты их поступления, профессиональная подготовка, повышение квалификации, стажировка); о занимаемой должности, дате назначения, переводах на иные должности и основаниях назначений (перевода), предыдущих местах работы; о заработной плате; об общем трудовом стаже, стаже педагогической деятельности; о прохождении аттестации, датах прохождения и принятых аттестационными комиссиями решениях и вынесенных рекомендациях; о награждении и поощрении; фотоизображения с целью обеспечения соблюдения трудового законодательства и иных нормативных правовых актов, содействия в трудоустройстве, обучении, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы, информирования о работе и обеспечения сохранности имущества.

Об ответственности за достоверность представленных сведений предупрежден(а).

С вышеуказанными персональными данными могут быть совершены следующие действия: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление и уничтожение персональных данных.

Данные сведения должны обрабатываться на средствах организационной техники, а также в письменном виде.

Настоящее согласие вступает в силу с момента его подписания на срок действия трудового договора и может быть отозвано путем подачи письменного заявления директору МКОУ «Воробьевская СОШ им. Н.Т.Воробьева».

Я также утверждаю, что ознакомлен(а) с возможными последствиями моего отказа дать письменное согласие на обработку и передачу персональных данных.

(фамилия, имя, отчество)_____
Подпись

« ____ » _____ 20 ____ г.

Приложение 2

ПИСЬМЕННОЕ СОГЛАСИЕ НА ПЕРЕДАЧУ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬЕЙ СТОРОНЕ

Я, _____,
ФИО работника

наименование документа, удостоверяющего личность _____ № документа _____
дата выдачи _____, кем выдан _____ -
проживающий по адресу _____
адрес проживания

в соответствии со статьей 7 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (с последующими изменениями) даю в МКОУ «Воробьевская СОШ им. Н.Т.Воробьева» согласие на передачу следующих категорий моих персональных данных и (или) моего _____ :
указать степень родства, ФИО

- 1) _____ ;
 - 2) _____ ;
 - 3) _____ для
- обработки в целях

_____ следующим лицам _____

(указать Ф.И.О. физического лица или наименование организации, которым передаются персональные данные, адрес)

Указанные персональные данные могут обрабатываться следующими способами _____

Настоящее согласие вступает в силу с момента его подписания, действует до _____ и может быть отозвано путем подачи письменного заявления директору Учреждения.

Я также подтверждаю, что ознакомлен(а) с юридическими последствиями моего отказа дать письменное согласие на передачу указанных персональных данных.

_____ (дата)

_____ (подпись)

**ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных**

Я, _____
(фамилия, имя отчество работника)

(должность)

предупрежден(а), что приказом директора от _____ № _____
« _____ » мне будет предоставлен допуск к
персональным данным _____.

С перечнем персональных данных, к обработке которых предоставлен допуск, ознакомлен(а).

Настоящим добровольно принимаю на себя обязательства:

- 1) не разглашать третьим лицам персональные данные, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей;
- 2) не передавать и не раскрывать третьим лицам персональные данные, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей;
- 3) в случае попытки третьих лиц получить от меня персональные данные, сообщать непосредственному директору Учреждения;
- 4) не использовать конфиденциальные сведения с целью получения выгоды;
- 5) выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных;
- 6) знакомиться только с теми документами, к которым получен доступ в силу исполнения своих служебных обязанностей;
- 7) после прекращения права на допуск к персональным данным не разглашать и не передавать третьим лицам известные мне персональные данные.

Я осведомлен(а), что разглашение конфиденциальных сведений влечет за собой ответственность, предусмотренную законодательством Российской Федерации.

(должность)

(подпись)

(расшифровка подписи)
