



Утверждено
на заседании
педагогического совета № 1
МБОУ СОШ №28
От 28.08.2017

Положение «Об обработке и защите персональных данных»

I. Общие положения

1.1. Настоящее «Положение Об обработке и защите персональных данных» (далее - Положение) разработано на основании следующих документов:

- 1.1.1. Конституция Российской Федерации (12 декабря 1993 года);
- 1.1.2. Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных». Страсбург, 28 января 1981 года;
- 1.1.3. Федеральный закон Российской Федерации от 19 декабря 2005 года №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- 1.1.4. Федеральный закон Российской Федерации от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации»;
- 1.1.5. Трудовой кодекс Российской Федерации;
- 1.1.6. Федеральный закон Российской Федерации от 29 декабря 2012 г. №273-ФЗ "Об образовании в Российской Федерации";
- 1.1.7. Федеральный закон Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных»;
- 1.1.8. Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 09 сентября 2000 года № Пр.-1895;
- 1.1.9. Указ Президента Российской Федерации от 06 марта 1997 года №188 «Перечень сведений конфиденциального характера» ;
- 1.1.10. Указ Президента Российской Федерации от 17 марта 2008 года №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- 1.1.11. Положение о методах и способах защиты информации в информационных системах персональных данных, утверждено приказом ФСТЭК России от 05 февраля 2010 года №58;
- 1.1.12. Требования к защите персональных данных при их обработке в информационных системах персональных данных, утверждены

постановлением Правительства Российской Федерации от 01 ноября 2012 г. №1119;

1.1.13. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждено постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687;

1.1.14. Порядок проведения классификации информационных систем персональных данных, утвержденный совместным приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года №55/86/20.

1.2. Настоящим Положением определяется порядок обработки, т.е. действий (операций) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение работников, обучающихся и их родителей (законных представителей) муниципального бюджетного общеобразовательного учреждения СОШ №28 города Ставрополя с использованием средств автоматизации или без использования таких средств. Положение устанавливает требования по защите персональных данных в информационных системах персональных данных.

II. Основные понятия и состав персональных данных

2.1. Цели обработки персональных данных:

2.1.1. Персональные данные обучающегося обрабатываются в целях воспитания и обучения обучающегося, обеспечения его личной безопасности, контроля качества образования, пользования льготами, предусмотренными законодательством Российской Федерации и локальными актами администрации.

2.1.2. Персональные данные работника обрабатываются с целью обеспечения трудовых отношений.

2.2. Основные термины и определения, применяемые в настоящем Положении:

2.2.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация о физическом лице.

2.2.2. Оператор - юридическое лицо, самостоятельно и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В рамках настоящего положения оператором является юридическое лицо – МБОУ СОШ №28 города Ставрополя.

2.2.3. К субъектам персональных данных (далее - субъекты) относятся лица, персональные данные которых переданы гимназии, (как на добровольной основе, так и в рамках выполнения требований нормативно - правовых актов) для обработки (в том числе передачи).

2.2.4. Работник - физическое лицо, состоящее в трудовых отношениях с Оператором.

2.2.5. Обучающийся - физическое лицо, проходящее обучение в гимназии.

2.2.6. Третье лицо - физическое либо юридическое лицо, которому Оператор на основании договора передает полностью или частично функции по обработке персональных данных.

2.2.7. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.2.8. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

2.2.9. Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.2.10. Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором 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.

2.2.11. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.2.12. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.2.13. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.2.14. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.2.15. Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем.

2.3. К персональным данным субъектов персональных данных относятся следующие сведения:

- ФИО;
- паспортные данные;
- дата и место рождения;
- гражданство;
- данные о регистрации;
- сведения об образовании;
- сведения о воинском учете;
- место жительства;
- ИНН, СНИЛС, номер страхового полиса;
- номер телефона (домашний, сотовый);
- семейное положение;
- сведения о зарплате, налогах;
- лицевой счет.

2.4. Документы, содержащие персональные данные, являются конфиденциальными.

III. Получение, обработка и хранение персональных данных

3.1. Получение персональных данных.

3.1.1. Оператор получает сведения о персональных данных субъектов персональных данных из следующих источников:

- паспорта или иного документа, удостоверяющего личность;
- анкет, заполняемых гражданами.

Субъект персональных данных обязан предоставлять достоверные сведения о себе.

3.1.2. Все персональные данные следует получать непосредственно от субъекта персональных данных. Субъект самостоятельно принимает решение о предоставлении своих персональных данных и дает письменное согласие (соглашение) на их обработку Оператором по форме согласно Приложению №1. В случае недееспособности либо несовершеннолетия субъекта персональных данных все персональные субъекта следует получать от его законных представителей. Законный представитель самостоятельно принимает решение о предоставлении персональных данных своего подопечного и дает письменное согласие на их обработку Оператором по форме согласно Приложению №2.

3.1.3. Условием обработки персональных данных субъекта персональных данных является его письменное согласие. Письменное Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

3.1.4. Письменное согласие вступает в силу с момента его подписания субъектом персональных данных (его законным/юридическим представителем) и действует до момента отзыва по решению суда или письменному решению самого субъекта персональных данных.

3.1.5. Согласия субъекта на обработку его персональных данных не требуется в следующих случаях:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для исполнения договора, стороной которого или поручителем по которому является субъект персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

3.1.6. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных в соответствии с положением статьи 9 Федерального закона № 152 «О персональных данных»

3.1.7. Запрещается получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни, о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.1.8. Проведение работ по сбору письменных соглашений граждан на обработку персональных данных между Оператором и субъектом персональных данных осуществляется уполномоченными локальным нормативным актом лицами и передается на хранение в личные дела сотрудников и учащихся.

3.1.9. Бланки письменных соглашений граждан подписанные со стороны Оператора передаются уполномоченным лицам, ответственным за сбор письменных соглашений граждан на обработку персональных данных (между Оператором и субъектом) и комиссии.

3.2. Хранение персональных данных.

3.2.1. Хранение персональных данных субъектов осуществляется бухгалтерией, учебной частью, социальной службой, психологом, библиотекой и иными структурными единицами на бумажных и электронных носителях с ограниченным доступом.

3.2.2. Личные дела хранятся в бумажном виде. Личные дела хранятся в специально отведенной секции архива (в опечатанном виде), что обеспечивает защиту от случайного или несанкционированного доступа.

3.2.3. Службы учреждения, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положению об особенностях обработки персональных

данных, осуществляемой без использования средств автоматизации», утвержденному постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687.

3.2.4. Хранение персональных данных в автоматизированной базе данных обеспечивается защитой от несанкционированного доступа согласно «Требованиям к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119

3.3. Передача персональных данных

3.3.1. При передаче персональных данных субъекта Оператор обязан соблюдать следующие требования:

3.3.1.1. не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами;

3.3.1.2. предупредить лиц, получающих персональные данные субъекта, 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 субъекта, обязаны соблюдать требования конфиденциальности;

3.3.1.3. не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;

3.3.1.4. передавать персональные данные субъекта представителям субъектов в порядке, установленном Трудовым Кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций.

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

3.4. Уничтожение персональных данных

3.4.1. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3.4.2. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном законодательством Российской Федерации.

IV. Права и обязанности сторон в области защиты персональных данных

4.1. Субъект персональных данных обязан:

- передать Оператору комплекс достоверных, документированных персональных данных;
- своевременно сообщать Оператору об изменении своих персональных данных.

4.2. Субъект персональных данных имеет право:

- на получение сведений об Операторе, о месте его нахождения, о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными за исключением случаев, если предоставление персональных данных нарушает конституционные права и свободы других лиц;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральными законами;
- получать информацию, касающуюся обработки его персональных данных;
- обжаловать в судебном порядке любые неправомерные действия или бездействие Оператора при обработке и защите персональных данных;
- требовать об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- требовать от Оператора исключения, исправления или уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональных данных являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- при отказе оператора исключить или исправить персональные данные субъекта заявить в письменной форме о своем несогласии с соответствующим обоснованием такого несогласия, при отклонении оператором указанного обращения (несогласия), обжаловать действия оператора в порядке, предусмотренном законодательством Российской Федерации.

4.3. Если обязанность предоставления персональных данных субъектом установлена федеральным законом (включая налоговое, трудовое право), Оператор обязан разъяснить субъекту персональные данные юридические последствия отказа предоставить свои персональные данные.

4.4. Оператор обязан безвозмездно предоставить субъекту персональных данных возможность ознакомления с персональными данными, относящимися к нему, а также внести в них необходимые изменения, уничтожить или заблокировать соответствующие персональные данные по предоставлению субъектом сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не

являются необходимыми для заявленной цели обработки. Сведения о персональных данных должны быть предоставлены субъекту в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

4.5. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа в установленные нормативно-правовыми актами Российской Федерации сроки.

4.6. В случае выявления недостоверных персональных данных или неправомерных действий с ними, Оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту, с момента получения такой информации на период проверки. В случае подтверждения факта недостоверности персональных данных, обрабатываемых Оператором, на основании соответствующих документов обязан уточнить персональных данных в течение 7 (семи) рабочих дней со дня их получения и снять их блокирование.

4.7. В случае выявления неправомерных действий с персональными данными, Оператор в срок, не превышающий 3 (трех) рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений, Оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных, Оператор обязан уведомить субъекта персональных данных или его законного представителя.

4.8. В случае достижения цели обработки персональных данных Оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий 30 (тридцати) рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором или иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

4.9. В случае отзыва субъектом согласия на обработку своих персональных данных Оператор обязан прекратить обработку персональных данных и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий 30 (тридцати) рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением сторон и (или) федеральным законом. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных. В случае невозможности уничтожения персональных данных в течение вышеуказанного срока Оператор должен осуществить блокирование таких персональных данных и обеспечить

уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

4.10. До начала обработки персональных данных Оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, установленных законодательством Российской Федерации.

4.11. Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации. Уведомление должно содержать следующие сведения:

- наименование (фамилия, имя, отчество), адрес Оператора;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональных данных которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых способов обработки персональных данных;
- описание мер, применяемых Оператором для обеспечения безопасности персональных данных, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и их контактные сведения;
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

V. Доступ персонала к обработке персональных данных

5.1. Внутренний доступ (доступ внутри учреждения) к персональным данным субъекта. Право доступа к персональным данным субъекта имеют: директор, главный бухгалтер, экономист, делопроизводитель, заместители директора (доступ к персональным данным субъектов в части их касающейся), учителя и классные руководители (доступ к информации, содержащейся в классных журналах тех классов, в которых он ведет занятия), социальный педагог, педагог-психолог, педагог дополнительного образования, учитель-логопед, заведующий библиотекой, врач, медицинская сестра, преподаватель-организатор ОБЖ (доступ к персональным данным субъектов в части их

касающейся), охранник (регистрация посещений учреждения, учет выдачи ключей).

5.2. Все сотрудники, имеющие доступ к персональным данным субъектов, обязаны подписать соглашение о неразглашении персональных данных, по форме согласно Приложению №3.

VI. Защита персональных данных

6.1. Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе деятельности Оператора.

6.2. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий, в соответствии с требованиями к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

6.3. Для защиты персональных данных Оператором применяются следующие принципы и правила:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей персональных данных;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудниками требований нормативно-методических документов по защите персональных данных;
- исключение бесконтрольного пребывания посторонних лиц в помещениях, в которых ведется обработка персональных данных и находится соответствующая вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушений требований разрешительной системы доступа;
- воспитательная и разъяснительная работа с сотрудниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- регулярное обучение работников по вопросам, связанным с обеспечением безопасности персональных данных;
- ограничение доступа к техническим средствам и системам обработки информации, на которых содержатся персональные данные;

- создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для лица, пытающегося совершить несанкционированный доступ и овладение информацией;
- резервирование защищаемых данных (создание резервных копий).

VII. Уничтожение персональных данных

7.1. В соответствии с нормативными актами РФ персональных данных должны быть уничтожены:

- при истечении срока хранения;
- по требованию субъекта персональных данных, в определенных законодательством РФ случаях;
- в случае выявления неправомерных действий с персональными данными и невозможности устранения допущенных нарушений;
- в случае достижения цели обработки персональных данных;
- в случае утраты необходимости достижения цели обработки.

Контроль сроков хранения, целей обработки персональных данных производится на основании допустимых сроков хранения и допустимых целей.

7.2. Решение об уничтожении персональных данных, организацию и проведение уничтожения принимают и осуществляют владельцы информационных систем персональных данных и процессов обработки персональных данных.

7.3. Об уничтожении персональных данных должен быть уведомлен субъект персональных данных.