

УТВЕРЖДАЮ

Директор муниципального бюджетного
общеобразовательного учреждения
«Средняя общеобразовательная школа
№ 7»



Т.В. Карелина
«28» августа 2020 года

**Политика МБОУ СОШ №7 г. о. Мытищи в отношении
обработки персональных данных сотрудников
учреждения, обучающихся и (или) родителей (законных
представителей)**

г. о. Мытищи 2020 г.

1. Общие положения

Политика определяет требования к порядку сбора, обработки, хранения, передачи и защиты ПДн физических лиц (далее Субъектов), реализуемые в МБОУ СОШ №7 (далее Учреждение)

Действие настоящей Политики распространяется на все процессы по работе с ПДн, как с использованием средств автоматизации, так и без использования таких средств. Целью настоящей Политики является соблюдение прав и свобод человека и гражданина при обработке его ПДн в информационных системах МБОУ СОШ №7, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

2. Правовые основания и цели обработки персональных данных

Настоящая Политика разработана на основании Конституции РФ. Гражданского Кодекса РФ. Трудового Кодекса РФ. и в соответствии с требованиями Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», Постановления Правительства РФ от 21.03.2012 N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Цель данной Политики - обеспечение прав граждан при обработке их персональных данных, и принятие мер от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных Субъектов.

МБОУ СОШ №7 осуществляет обработку персональных данных только в целях, непосредственно связанных с деятельностью учреждения, в частности для:

- обеспечение процесса ведения электронного журнала;
- взаимодействия законных представителей и учащихся с преподавателями в электронном виде;
- информирования об успеваемости учащегося и ходе учебного процесса;
- предоставления образовательных услуг;
- проведения олимпиад, консультационных семинаров;
- направления работ сотрудников (учащихся, воспитанников) на конкурсы;
- дистанционного обучения;
- ведения сайта ОУ;
- автоматизации работы библиотеки;
- проведения мониторинга деятельности школы
- организации кадрового учета сотрудников школы, ведения кадрового делопроизводства, в соответствии с Трудовым кодексом РФ, федеральными законами.

Учреждение собирает данные только в объеме, необходимом для достижения выше названных целей.

Передача третьим лицам персональных данных без письменного согласия не допускается.

Режим конфиденциальности персональных данных снимается в случаях обезличивания или включения их в общедоступные источники персональных данных, если иное не определено законом.

Сотрудники, в обязанность которых входит обработка персональных данных Субъекта, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом, а также настоящей Политикой.

Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской

Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

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.

Настоящая политика утверждается Директором Учреждение и является обязательной для исполнения всеми сотрудниками, имеющими доступ к персональным данным Субъекта.

3. Обрабатываемые категории персональных данных и источники их поступления

Персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому Субъекту.

Учреждение обрабатывает персональные данные следующих категорий субъектов персональных данных:

- *персональные данные сотрудника школы - информация, необходимая в связи с трудовыми отношениями и касающиеся конкретного работника.*
- *персональные данные Учащихся, их законных представителей и сотрудников Учреждения - информация, необходимая для достижения целей обработки и для выполнения требований законодательства Российской Федерации.*

К персональным данным Субъекта, которые, обрабатывает Учреждение, относятся:

3.1. Несовершеннолетних до 14 лет:

- Данные об успеваемости (оценки и посещаемость) Обучающегося.
- Данные о домашних заданиях, расписании Обучающегося.
- Фамилия/Имя/Отчество Обучающегося и законного представителя.
- Гражданство Обучающегося и законного представителя.
- СНИЛС Обучающегося и законного представителя.
- Данные документа, удостоверяющего личность, включая паспортные данные (серия, номер, дата выдачи, кем выдан) Обучающегося и законного представителя.
- Информация о визе Обучающегося и законного представителя.
- Медицинская группа здоровья обучающегося.
- Физкультурная группа здоровья обучающегося.
- Дата рождения Обучающегося и законного представителя.
- Место рождения Обучающегося и законного представителя.
- Пол Обучающегося и законного представителя.
- Номер мобильного телефона Обучающегося и законного представителя. 1
- Адрес электронной почты (email) Обучающегося и законного представителя.

3.2. Несовершеннолетних от 14 лет:

- Фамилия/Имя/Отчество.
- Гражданство.
- СНИЛС.
- Данные документа, удостоверяющего личность, включая паспортные данные (серия, номер, дата выдачи, кем выдан).
- Информация о визе.
- Медицинская группа здоровья.
- Физкультурная группа здоровья.
- Дата рождения.
- Место рождения.

- Пол.
- Номер мобильного телефона.
- Адрес электронной почты (email).
- Данные об успеваемости (оценки и посещаемость) Обучающегося.
- Данные о домашних заданиях, расписании Обучающегося.

3.3. Для совершеннолетних:

- Фамилия/Имя/Отчество
- Гражданство.
- СНИЛС.
- Данные документа, удостоверяющего личность, включая паспортные данные (серия, номер, дата выдачи, кем выдан).
- Информация о визе.
- Медицинская группа здоровья.
- Физкультурная группа здоровья.
- Дата рождения.
- Место рождения.
- Пол.
- Номер мобильного телефона.
- Адрес электронной почты (email).
- Данные об успеваемости (оценки и посещаемость) Обучающегося.
- Данные о домашних заданиях, расписании Обучающегося.

3.4. Для родителей (законных представителей):

- Фамилия/Имя/Отчество.
- Гражданство.
- СНИЛС.
- Данные документа, удостоверяющего личность, включая паспортные данные (серия, номер, дата выдачи, кем выдан).
- Информация о визе.
- Дата рождения.
- Место рождения.
- Пол.
- Номер мобильного телефона.
- Адрес электронной почты (email).

3.5. Для сотрудников:

- Фамилия/Имя/Отчество.
- Гражданство.
- СНИЛС.
- Данные документа, удостоверяющего личность, включая паспортные данные (серия, номер, дата выдачи, кем выдан).
- Информация о визе.
- Дата рождения.
- Место рождения.
- Пол.
- Должность и квалификация.
- Номер мобильного телефона.
- Адрес электронной почты (email).
- Образование.

- Педагогический стаж.
- Тип занятости.

3.6. Иная необходимая информация, которую Субъект добровольно сообщает о себе для получения услуг предоставляемых Учреждением, если ее обработка не запрещена законом.

4. Основные принципы обработки, передачи и хранения персональных данных

Обработка персональных данных - любое действие (операция) или совокупность действий, 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.

Учреждение ведет обработку персональных данных Субъекта с использованием средств автоматизации (автоматизированная обработка), и без использования таких средств (неавтоматизированная обработка).

Обработка персональных данных должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Учреждения;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
- уничтожения персональных данных после достижения целей обработки или в случае утраты необходимости в их достижении;
- личной ответственности сотрудников Учреждения за сохранность и конфиденциальность персональных данных, а также носителей этой информации.

Обязанности Учреждения

В целях обеспечения прав и свобод человека и гражданина Учреждение при обработке персональных данных Субъекта обязано соблюдать следующие общие требования:

- обработка персональных данных Субъекта может осуществляться исключительно в целях оказания законных услуг Субъектам;
- персональные данные Субъекта следует получать у него самого. Если персональные данные Субъекта возможно получить только у третьей стороны, то Субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Сотрудники Учреждения должны сообщить Субъектам о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа Субъекта дать письменное согласие на их получение;
- учреждение не имеет права получать и обрабатывать персональные данные о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, за исключением случаев, предусмотренных законом. В частности, вправе обрабатывать указанные персональные данные Субъекта только с его письменного согласия;

- предоставлять Субъекту или его представителю информацию о наличии персональных данных, относящихся к соответствующему Субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении Субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса Субъекта персональных данных или его представителя;
- хранение и защита персональных данных Субъекта от неправомерного их использования или утраты обеспечивается учреждением, за счет его средств в порядке, установленном действующим законодательством РФ;
- в случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу Субъекта либо уполномоченного органа по защите прав субъектов персональных данных Учреждение обязано осуществить блокирование персональных данных на период проверки;
- в случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных Субъектом либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование;
- в случае достижения цели обработки персональных данных Учреждение обязано незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней, и уведомить об этом Субъекта, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган;
- в случае отзыва Субъектом согласия на обработку своих персональных данных учреждение обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней, если иное не предусмотрено соглашением между Учреждением и Субъектом. Об уничтожении персональных данных Учреждение обязано уведомить Субъекта.

5. Меры по обеспечению безопасности персональных данных при их обработке

5.1 Перечень персональных данных, подлежащих защите в Учреждении, формируется в соответствии с ФЗ РФ от 27 июля 2006 г. № 152 - ФЗ «О персональных данных». Сведениями, составляющими персональные данные, является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Учреждение предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

В целях координации действий по обеспечению безопасности персональных данных в Учреждении назначаются ответственные за обеспечение безопасности персональных данных.

Персональные данные Субъекта могут быть предоставлены третьим лицам только с письменного согласия Субъекта.

Доступ Субъекта к своим персональным данным предоставляется при обращении либо при получении запроса Субъекта. Учреждение обязано сообщить Субъекту информацию о наличии персональных данных о нем, а также предоставить возможность ознакомления с ними в течение тридцати рабочих дней с момента обращения или получения запроса.

Запрос должен содержать номер основного документа, удостоверяющего личность Субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись Субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

Клиент имеет право на получение при обращении или при отправлении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Учреждением, а также цель такой обработки;
- способы обработки персональных данных, применяемые Учреждением;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для Субъекта может повлечь за собой обработка его персональных данных.

Сведения о наличии персональных данных должны быть предоставлены Субъекту в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Право Субъекта на доступ к своим персональным данным ограничивается в случае, если предоставление персональных данных нарушает конституционные права и свободы других лиц.

5.2. 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 технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе деятельности Учреждения.

Регламентация доступа персонала к документам и базам данных с персональными сведениями входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами Учреждения. Для защиты персональных данных Субъектов необходимо соблюдать ряд мер:

- осуществление пропускного режима в служебные помещения;
- назначение должностных лиц, допущенных к обработке ПД;
- хранение ПД на бумажных носителях в охраняемых или запираемых помещениях, сейфах, шкафах;
- наличие необходимых условий в помещениях для работы с документами и базами данных с персональными сведениями; в помещениях, в которых находится вычислительная техника;
- организация порядка уничтожения информации;
- ознакомление работников, непосредственно осуществляющих обработку ПД, с требованиями законодательства РФ в сфере ПД, локальными актами оператора в сфере ПД и обучение указанных работников;
- осуществление обработки ПД в автоматизированных информационных системах на рабочих местах с разграничением полномочий, ограничение доступа к рабочим местам, применение механизмов идентификации доступа по паролю и электронному ключу, средств криптозащиты;

- осуществление внутреннего контроля соответствия обработки ПД требованиям законодательства.

Для защиты персональных данных 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 школы, посетители, работники 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 Субъектов необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- технические средства охраны, сигнализации;
- порядок охраны помещений;
- требования к защите информации, предъявляемые соответствующими нормативными документами.

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

5.3. Ответственность за разглашение персональных данных и нарушение

Учреждение ответственно за персональную информацию, которая находится в его распоряжении и закрепляет персональную ответственность сотрудников за соблюдением, установленных в организации принципов уважения приватности.

Каждый сотрудник Учреждения, получающий для работы доступ к материальным носителям персональным данным, несет ответственность за сохранность носителя и конфиденциальность информации.

Учреждение обязуется поддерживать систему приема, регистрации и контроля рассмотрения жалоб Субъектов, доступную с помощью телефонной, телеграфной или почтовой связи.

Любое лицо может обратиться к сотруднику Учреждения с жалобой на нарушение данной Политики. Жалобы и заявления по поводу соблюдения требований обработки данных рассматриваются в течение тридцати рабочих дней с момента поступления.

Сотрудники Учреждения обязаны на должном уровне обеспечивать рассмотрение запросов, заявлений и жалоб Субъектов, а также содействовать исполнению требований компетентных органов. Лица, виновные в нарушении требований настоящей политики, привлекаются к дисциплинарной ответственности.

6. Права субъектов персональных данных

- Право на доступ к информации о самом себе.
- Право на определение форм и способов обработки персональных данных.
- Право на отзыв согласия на обработку персональных данных.
- Право ограничивать способы и формы обработки персональных данных, запрет на распространение персональных данных без его согласия.
- Право требовать изменение, уточнение, уничтожение информации о самом себе.
- Право обжаловать неправомерные действия или бездействия по обработке персональных данных и требовать соответствующей компенсации в суде.
- Право на дополнение персональных данных оценочного характера заявлением, выражающим его собственную точку зрения.

- Право определять представителей для защиты своих персональных данных.
- Право требовать от Учреждения уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные Субъекта, обо всех произведенных в них изменениях или исключениях из них.

7. Сроки обработки (хранения) персональных данных

Сроки обработки персональных данных определяются в соответствии со сроком обучения Учащегося в Учреждении, и сроком трудового договора Сотрудника.

8. Уточнение, блокирование и уничтожение персональных данных

Блокирование ПДн - это вспомогательный процесс. Он позволяет остановить обработку данных в случаях:

- выявления недостоверных персональных данных;
- выявления неправомерных действий с ними оператора;
- достижения цели обработки персональных данных;
- отзыва субъектом персональных данных согласия на обработку его персональных данных.

Во время блокирования происходит уточнение данных, устранение неправомерных действий с персональными данными или уничтожения персональных данных.

Осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, оператор обязан:

- при обращении или по запросу субъекта персональных данных;
- его законного представителя;
- уполномоченного органа по защите прав субъектов персональных данных;
- по требованию лица, по поручению которого обрабатываются персональные данные.

Блокирование производится с момента обращения или получения запроса на период проверки.

Блокирование персональных данных включает:

- прекращения сбора;
- систематизации;
- записи;
- накопления;
- уточнения;
- извлечения;
- использования;
- обезличивания;
- удаления;
- распространения персональных данных, в том числе их передачи.

С этой целью оператор должен обеспечить, прежде всего, идентификацию субъекта ПДн и далее поставить запрет на чтение и запись данных о субъекте в ИСПДн. При обращении к заблокированным данным о субъекте (например, с целью извлечения информации) рекомендуется выдача ИСПДн сообщения: «субъект заблокирован». Наиболее сложным является идентификация субъекта, так как в ИСПДн могут находиться неполные данные о субъекте (например, только фамилия и имя) или данные с ошибками. В таких случаях (нет 100% уверенности, что данные в ИСПДн относятся к субъекту) рекомендуется отказаться от блокирования в связи с невозможностью идентификации субъекта по данным в ИСПДн.

9. Заключительные положения

Настоящая Политика является документом, разработанным Учреждением, является общедоступной и подлежит размещению на официальном сайте.

Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

Контроль исполнения требований настоящей Политики осуществляется ответственными за обеспечение безопасности персональных данных Учреждения.

Ответственность должностных лиц Учреждения, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Учреждения.