

Рассмотрено  
Управляющим Советом  
протокол № 1 от 30.08.2018 г.

Утверждено приказом  
№ 369 от 31.08.2018 г.

## **Положение о персональных данных работников в муниципальном бюджетном общеобразовательном учреждении средней общеобразовательной школе №4**

### **1. Общие положения.**

1.1. Настоящее Положение устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников и учащихся МБОУ СОШ №4 (далее – Школа).

1.2. Цель разработки настоящего Положения – определение порядка обработки персональных данных работников и учащихся Школы; защита персональных данных работников и учащихся Школы от несанкционированного доступа и разглашения или утраты.

1.3. Настоящее Положение разработано на основании Конституции РФ, Трудового кодекса РФ, Кодекса РФ об административных правонарушениях, Гражданского кодекса РФ, Уголовного кодекса РФ, Федерального закона "Об информации, информатизации и защите информации", Устава и Правил внутреннего трудового распорядка Школы.

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

1.5. 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.

### **2. Понятие и состав персональных данных.**

2.1. Под персональными данными работников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. Под персональными данными учащихся понимается информация, необходимая работникам Школы в связи с образовательной (учебной и воспитательной) деятельностью, трудовыми отношениями и касающаяся конкретного ученика, а также сведения о фактах, событиях и обстоятельствах жизни учащегося, позволяющие идентифицировать его личность

2.3. Состав персональных данных (данные документы являются конфиденциальными):

- дата рождения;
- место рождения;
- гражданство;
- адрес регистрации;
- адрес места жительства;
- дата регистрации по месту;
- номер телефона (домашнего, личного сотового);
- семейное положение, состав семьи;
- фамилия, имя отчество членов семьи;

- число, месяц, год рождения, место рождения, гражданство членов семьи;
- паспортные данные (номер, серия паспорта, код региона, дата выдачи, кем выдан);
- информация о трудовой деятельности (периоды, наименование работодателя, должность (профессия));
- номер страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- сведения о воинском учете;
- образование;
- профессия;
- информация о наличии почетных званий, наград;
- информация о спортивных званиях, разрядах;
- информация о дисциплинарных взысканиях, поощрениях;
- информацию о состоянии здоровья;
- информацию о наличии судимости;
- личная фотография;
- информация о педагогическом и общем трудовом стаже;
- информация о предыдущем месте работы;
- информация о заработной плате сотрудника;
- информация о социальных льготах;
- специальность;
- занимаемая должность;
- содержание трудового договора;
- подлинники и копии приказов по личному составу и основания к приказам;
- личные дела и трудовые книжки сотрудников;
- информация по повышению квалификации и переподготовке сотрудников, их аттестации и прочим исследованиям;
- копии отчетов, направляемые в органы статистики;
- копии документов об образовании;
- рекомендации, характеристики и т.п.

2.4. Документы, указанные в п. 2.3. настоящего Положения, являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

### **3. Получение, обработка, передача и хранение персональных данных.**

3.1. Под обработкой персональных данных работника (учащегося) понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

3.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника (учащегося) обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных работника (учащегося) может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2.2. При определении объема и содержания обрабатываемых персональных данных работника (учащегося) директор школы должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными федеральными законами.

3.2.3. Получение персональных данных может осуществляться как путем представления их самим работником (учащимся), так и путем получения их из иных источников.

3.2.4. Персональные данные следует получать у самого работника (учащегося). 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. Директор школы должен сообщить работнику (учащемуся) о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника (учащегося) дать письменное согласие на их получение.

3.2.5. Директор школы не имеет права получать и обрабатывать персональные данные работника (учащегося) Школы о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, частной жизни, состоянии здоровья. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации и ст. 88 Трудового кодекса Российской Федерации, работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

3.2.6. Директор школы не имеет право получать и обрабатывать персональные данные работника (учащегося) о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.3. К обработке, передаче и хранению персональных данных работника (учащегося) могут иметь доступ сотрудники: (директор Школы (лицо, исполняющее обязанности), заместитель директора, главный бухгалтер, лицо, отвечающее за работу с кадрами, тьютор (классный руководитель), социальный педагог).

3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.5. Обработка персональных данных работников (учащегося) возможна без их согласия в следующих случаях:

3.5.1. персональные данные являются общедоступными;

3.5.2. персональные данные относятся к состоянию здоровья работника (учащегося) и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника (учащегося) невозможно;

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

3.6. Согласие работника (учащегося) не требуется в следующих случаях:

3.6.1. обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

3.6.2. обработка персональных данных осуществляется в целях исполнения трудового договора;

3.6.3. обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

3.6.4. обработка, предоставление персональных данных в связи с проведением единого государственного экзамена.

3.7. Передача персональных данных работника (учащегося) возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.

3.7.1. При передаче персональных данных работника (учащегося) директор школы должен соблюдать следующие требования:

- не сообщать персональные данные работника (учащегося) третьей стороне без письменного согласия работника (учащегося), 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 (учащегося) в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника (учащегося), 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 (учащегося), обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников (учащихся) в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным работников (учащихся) только специально уполномоченным лицам, определенным приказом по школе, 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;
- передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3.7.2. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

3.7.3. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.

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

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

3.8. Хранение и использование персональных данных работников (учащихся).

3.8.1. Персональные данные работников обрабатываются и хранятся в бухгалтерии школы и лица, ответственного за работу с кадрами.

3.8.2. Персональные данные работников (учащихся) могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде: в виде файлов в локальной компьютерной сети.

3.8.3. При получении персональных данных не от работника (за исключением случаев, если персональные данные были предоставлены работодателю на основании федерального закона или если персональные данные являются общедоступными) работодатель до начала обработки таких персональных данных обязан предоставить работнику следующую информацию: наименование (фамилия, имя, отчество) и адрес оператора или его представителя; цель обработки персональных данных и ее правовое основание; предполагаемые пользователи персональных данных; права субъекта персональных данных.

#### **4. Доступ к персональным данным сотрудника.**

4.1. Внутренний доступ (доступ внутри Школы). Право доступа к персональным данным работника (учащегося) имеют:

4.1.1. Директор школы (лицо, исполняющее обязанности);

4.1.2. Заместители директора в пределах, определенных должностными инструкциями;

4.1.3. Лицо, отвечающее за работу с кадрами;

4.1.4. Классный руководитель, социальный педагог; психолог

4.1.5. сам работник (учащийся), носитель данных.

4.2. Внешний доступ. Персональные данные вне Школы могут представляться в государственные и негосударственные функциональные структуры:

4.2.1. налоговые инспекции;

4.2.2. правоохранительные органы;

4.2.3. органы статистики;

4.2.4. страховые агентства;

4.2.5. военкоматы;

4.2.6. органы социального страхования;

4.2.7. пенсионные фонды;

4.2.8. подразделения муниципальных органов управления.

4.2.9. Другие организации. Сведения о работнике (в том числе, уволенном) могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника.

4.2.10. Родственники и члены семей. Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника.

## **5. Защита персональных данных работников.**

5.1. В целях обеспечения сохранности и конфиденциальности персональных данных работников (учащихся) Школы все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только лицами, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

5.2. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке предприятия и в том объеме, который позволяет не разглашать излишний объем персональных сведений о работниках (учащихся) школы.

5.3. Передача информации, содержащей сведения о персональных данных работников Школы, по телефону, факсу, электронной почте без письменного согласия работника запрещается.

5.4. Документы, содержащие персональные данные работников, хранятся в запирающихся шкафах и сейфах, обеспечивающих защиту от несанкционированного доступа.

5.5. Персональные компьютеры, в которых содержатся персональные данные, защищены паролями доступа.

5.6. Если работник (учащийся) считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона или иным образом нарушает его права и свободы, работник (учащийся) вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

5.7. В случае отзыва работником (учащимся) согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить работника (учащихся).

## **6. Ответственность за разглашение информации, связанной с персональными данными работника.**

6.1. 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.

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 4

ПРИКАЗ

От 12.08.2016 г.

г. Светлоград

№ 348

«О назначении АИБ и допуске работников школы к обработке персональных данных в 2016-2017 учебном году, утверждении нормативной документации»

В соответствии с Федеральным законом РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных», в дополнение к списку сотрудников, указанных в положении о работе с персональными данными работников и обучающихся МБОУ СОШ № 4 г. Светлограда для обеспечения выполнения своих функций

ПРИКАЗЫВАЮ:

1. Назначить администратором информационной безопасности (АИБ) МБОУ СОШ № 4 ответственного за обеспечение безопасности персональных данных (далее - ПДн) Кузьмина А.И.
2. Допустить к обработке персональных данных работников и обучающихся, ответственного за ведение воинского учета преподавателя ОБЖ Товстолицкого И.В.
3. Допустить к обработке персональных данных обучающихся ответственного за организацию питания Слюсареву С.Г.
4. Допустить к обработке персональных данных обучающихся педагогов - психолога Арутюнян Л.В., социального педагога Дьякову О.С., психолога Бурлуцкую Е.Н.
5. Допустить к обработке персональных данных сотрудников школы: заместителя директора по АХЧ Мельцаеву И.И., секретаря-делопроизводителя Кабилкину С.В., специалиста по кадрам и охране труда Черкашину Г.Д., инженера Кузьмина А.И.
6. Допустить к обработке персональных данных обучающихся и сотрудников школы заместителя директора по УВР Панихидкину Н.И., заместителя директора по УВР Калашникову И.С., заместителя директора по УВР Кущенко Н.Н. заместителя директора по УВР Таранец А.Н., заместителя директора по ВР Мочалкину Ю.П., классных руководителей.
7. Указанным лицам в своей деятельности при работе с персональными данными руководствоваться Федеральным законом РФ от 27 июля 2006

- года № 152-ФЗ «О персональных данных», Положением о работе с персональными данными работников и обучающихся МБОУ СОШ № 4 г. Светлограда.
8. Утвердить Порядок доступа сотрудников МБОУ СОШ № 4 в помещения, в которых ведется обработка персональных данных (Приложение №1)
  9. Утвердить Согласие субъекта (законного представителя) на обработку персональных данных (Приложение №2)
  10. Утвердить форму журнала учета мероприятий по обеспечению и контролю безопасности ПДн, обрабатываемых в МБОУСОШ №4 (Приложение №3)
  11. Утвердить инструкцию Администратора безопасности МБОУ СОШ№4 (Приложение №4)
  12. Утвердить соглашение о неразглашении информации, содержащей персональные данные (Приложение №5)
  13. Утвердить План внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБОУСОШ №4 на 2016-2017 уч. год (Приложение №6)
  14. Утвердить Политику в области обработки и обеспечения безопасности персональных данных в информационных системах персональных данных МБОУ СОШ №4 (Приложение №7).
  15. Утвердить Регламент осуществления внутреннего контроля за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в информационных системах персональных данных МБОУ СОШ № 4 (Приложение №8).
  16. Утвердить состав постоянно действующей комиссии по проверки за безопасностью работы с персональными данными в следующем составе:  
Председатель комиссии Кузьминов А.И.  
Члены комиссии  
Кущенко Н.Н. – заместитель директора по УВР  
Черкашина Г.Д. – специалист по ОТ  
Панихидкина Н.И. – заместитель директора по УВР  
Мишура А.В. –учитель информатики
  17. Утвердить положение «О порядке уничтожения персональных данных» (Приложение № 9).
  18. Контроль за исполнением настоящего приказа оставляю за собой.

Директор муниципального бюджетного  
общеобразовательного учреждения  
средней общеобразовательной школы № 4:

И.В. Краснова





**Порядок  
доступа сотрудников МБОУ СОШ № 4.  
в помещения, в которых ведется обработка персональных данных.**

1. Настоящий Порядок доступа сотрудников МБОУ СОШ № 4 в помещения, в которых ведется обработка персональных данных (далее – Порядок) разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 152 ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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» и другими нормативными правовыми актами.

2. Персональные данные относятся к конфиденциальной информации. Должностные лица МБОУ СОШ № 4, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе, установлением правил доступа в помещения, где обрабатываются персональные данные в информационной системе персональных данных и без использования средств автоматизации.

4. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется в охраняемых помещениях. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

5. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только работники МБОУ СОШ № 4 уполномоченные на обработку персональных данных приказом директора.

6. Ответственными за организацию доступа в помещения МБОУ СОШ № 4, в которых ведется обработка персональных данных, являются директор МБОУ СОШ № 4.

7. Нахождения лиц в помещениях МБОУ СОШ № 4, не являющихся уполномоченными лицами на обработку персональных данных, возможно только в сопровождении работника МБОУ СОШ № 4 на время, ограниченное необходимостью решения вопросов, связанных с исполнением определенных функций и (или) осуществлением полномочий в рамках договоров, заключенных с МБОУ СОШ № 4.

8. Регистрация посетителей МБОУ СОШ № 4 осуществляется уполномоченными на ведение делопроизводства сотрудниками МБОУ СОШ № 4 с обязательной отметкой в журнале регистрации.

9. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, проводится лицом ответственным за организацию обработки персональных данных или комиссией, назначенной приказом директора МБОУ СОШ № 4.

**СОГЛАСИЕ СУБЪЕКТА  
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Я, \_\_\_\_\_,  
(Ф.И.О.)

проживающий по адресу: \_\_\_\_\_

Паспорт № \_\_\_\_\_, выданный \_\_\_\_\_ (кем \_\_\_\_\_ и  
когда) \_\_\_\_\_

настоящим даю свое согласие на обработку моих персональных данных, к которым относятся:

- дата рождения;
- место рождения;
- гражданство;
- адрес регистрации;
- адрес места жительства;
- дата регистрации по месту;
- номер телефона (домашнего, личного сотового);
- семейное положение, состав семьи;
- фамилия, имя отчество членов семьи;
- число, месяц, год рождения, место рождения, гражданство членов семьи;
- паспортные данные (номер, серия паспорта, код региона, дата выдачи, кем выдан);
- информация о трудовой деятельности (периоды, наименование работодателя, должность (профессия));
- номер страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- сведения о воинском учете;
- образование;
- профессия;
- информация о наличии почетных званий, наград;
- информация о спортивных званиях, разрядах;
- информация о дисциплинарных взысканиях, поощрениях;
- информацию о состоянии здоровья;
- информацию о наличии судимости;
- личная фотография;
- информация о педагогическом и общем трудовом стаже;
- информация о предыдущем месте работы;
- информация о заработной плате сотрудника;
- информация о социальных льготах;
- специальность;
- занимаемая должность;
- содержание трудового договора;
- подлинники и копии приказов по личному составу и основания к приказам;
- личные дела и трудовые книжки сотрудников;
- информация по повышению квалификации и переподготовке сотрудников, их аттестации и прочим исследованиям;
- копии отчетов, направляемые в органы статистики;
- копии документов об образовании;

- рекомендации, характеристики и т.п.

Я даю согласие на использование моих персональных данных в целях

---

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу третьим лицам), обезличивание, блокирование, трансграничную передачу персональных данных, а также осуществление любых иных действий с моими персональными данными, предусмотренных действующим законодательством Российской Федерации.

МБОУ СОШ №4 гарантирует, что обработка моих личных данных осуществляется в соответствии с действующим законодательством Российской Федерации.

Я проинформирован, что МБОУ СОШ № 4 будет обрабатывать мои персональные данные как неавтоматизированным, так и автоматизированным способом обработки.

Данное Согласие действует до достижения целей обработки моих персональных данных, установленных действующим законодательством Российской Федерации.

Согласие может быть отозвано по моему письменному заявлению.

Я подтверждаю, что, давая такое Согласие, я действую своей волей и в своих интересах.

Дата: \_\_\_\_\_ Подпись \_\_\_\_\_ / \_\_\_\_\_ /

**СОГЛАСИЕ ЗАКОННОГО ПРЕДСТАВИТЕЛЯ  
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОДОПЕЧНОГО**

Я, \_\_\_\_\_,  
(Ф.И.О.)

Проживающий по адресу: \_\_\_\_\_

Паспорт № \_\_\_\_\_, выданный \_\_\_\_\_ (кем \_\_\_\_\_ и  
когда) \_\_\_\_\_

как законный представитель на основании \_\_\_\_\_ (документ, подтверждающий, что  
субъект \_\_\_\_\_ является \_\_\_\_\_ законным \_\_\_\_\_ представителем  
подопечного) \_\_\_\_\_

настоящим даю свое согласие на обработку в (наименование и юридический адрес  
оператора) персональных данных своего подопечного \_\_\_\_\_  
(дата рождения) \_\_\_\_\_, к которым относятся:

данные свидетельства о рождении;  
данные медицинской карты;  
адрес проживания подопечного;  
прочие сведения.

Я даю согласие на использование персональных данных своего подопечного в целях:  
обеспечения учебного процесса подопечного;  
медицинского обслуживания;  
ведения статистики.

Настоящее согласие предоставляется на осуществление любых действий в отношении персональных данных моего подопечного, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу третьим лицам – районным медицинским учреждениям, военкомату, отделениям милиции и т.д.), обезличивание, блокирование, трансграничную передачу персональных данных, а также осуществление любых иных действий с моими персональными данными, предусмотренных действующим законодательством РФ.

МБОУ СОШ № 4 гарантирует, что обработка персональных данных осуществляется в соответствии с действующим законодательством РФ.

Я проинформирован, что МБОУ СОШ № 4 будет обрабатывать персональные данные как неавтоматизированным, так и автоматизированным способом обработки.

Данное Согласие действует до достижения целей обработки персональных данных подопечного в МБОУ СОШ № 4.

Согласие может быть отозвано по моему письменному заявлению.

Я подтверждаю, что, давая такое Согласие, я действую своей волей и в интересах своего подопечного.

Дата: \_\_\_\_\_ Подпись \_\_\_\_\_ / \_\_\_\_\_ /

**ЖУРНАЛ  
УЧЕТА МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ И КОНТРОЛЮ БЕЗОПАСНОСТИ ПДН, ОБРАБАТЫВАЕМЫХ  
В МБОУСОШ №4**

Журнал начат « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.  
Должность \_\_\_\_\_ / ФИО должностного лица /

Журнал завершен « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.  
Должность \_\_\_\_\_ / ФИО должностного лица /

№ п/п	Наименование мероприятия, основание для проведения	Описание мероприятия	Сроки проведения контрольных мероприятий		Состав участников	Объекты контроля	Выявленные нарушения, выданные рекомендации	Отметка о контроле устранения выявленных нарушений
			Дата начала	Дата окончания				





## **ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ**

### **МБОУ СОШ № 4**

#### **1. ОБЩИЕ ПОЛОЖЕНИЯ**

Администратор безопасности МБОУ СОШ № 4 за обеспечение безопасности персональных данных (далее - ПДн) назначается руководителем, на основании приказа из числа работников школы МБОУ СОШ № 4. В своей работе Администратор информационной безопасности (далее - АИБ) руководствуется законодательством Российской Федерации в области обеспечения безопасности ПДн, руководящими и нормативными документами ФСТЭК России и ФСБ России, а так же организационно-распорядительными документами МБОУ СОШ № 4. Администратор безопасности является ответственным должностным лицом МБОУ СОШ № 4, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты информационных систем персональных данных (далее – ИСПДн) и их ресурсов. Требования администратора информационной безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

Администратор безопасности должен иметь специальное рабочее место, размещенное в школе так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты, подключением к ИСПДн, а так же средствами контроля за техническими средствами защиты.

#### **2. Должностные обязанности**

##### **2.1. Обязанности администратора безопасности:**

2.1.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.1.2. Осуществлять установку, настройку и сопровождение средств защиты информации (далее - СЗИ).

2.1.3. Участвовать в контрольных и тестовых испытаниях, и проверках элементов ИСПДн.

2.1.4. Участвовать в приемке новых программных средств.

2.1.5. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

2.1.6. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.

2.1.7. Вести контроль над процессом осуществления резервного копирования объектов защиты.

2.1.8. Осуществлять выполнение мероприятий по осуществлению внутреннего контроля за обеспечением уровня защищенности ПДн и соблюдением условий использования СЗИ, а также соблюдением требований законодательства Российской Федерации по обработке ПДн в ИСПДн.

2.1.9. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

2.1.10. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.1.11. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.1.12. Контролировать в рамках своих полномочий исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты, в том числе на основании Порядка обеспечения антивирусной защиты ИСПДн и Порядка обеспечения парольной защиты ИСПДн, утвержденных регламентом обеспечения безопасности ПДн, обрабатываемых в ИСПДн.

2.1.13. Контролировать исполнение пользователями парольной политики.

2.1.14. Контролировать работу пользователей в сетях общего пользования.

2.1.15. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.

2.1.16. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.1.17. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.

2.1.18. Периодически представлять руководству отчет о состоянии защиты ИСПДн, о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

#### 2.2. Права администратора безопасности персональных данных:

2.2.1. Не допускать к работе на элементах ИСПДн лиц, не получивших в установленном порядке право доступа к персональным данным, обрабатываемым в ИСПДн.

2.2.2. Участвовать в периодических контрольных проверках состояния защищённости тиражируемых объектов ИСПДн, рабочих станций пользователей и тестирования правильности функционирования средств защиты ИСПДн.

2.2.3. Обращаться к ответственному за организацию обработки персональных данных с предложениями по усовершенствованию системы защиты персональных данных ИСПДн.

2.2.4. Принимать необходимые меры по оперативному реагированию, в случае возникновения внештатной ситуации, с целью ликвидации ее последствий.

Директор школы

И.В.Краснова

С инструкцией ознакомлен (а) \_\_\_\_\_

(дата)

\_\_\_\_\_

(подпись)

\_\_\_\_\_

(расшифровка подписи)

инструкцию получил (а): \_\_\_\_\_

(дата)

\_\_\_\_\_

(подпись)

\_\_\_\_\_

(расшифровка подписи)

\_\_\_\_\_

(личная подпись)

« \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**СОГЛАШЕНИЕ  
О НЕРАЗГЛАШЕНИИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ  
ДАННЫЕ**

Я, \_\_\_\_\_,  
(Ф.И.О.)

Проживающий по адресу: \_\_\_\_\_

Паспорт № \_\_\_\_\_, выданный (кем и когда) \_\_\_\_\_

предупрежден (а) о том, что на период исполнения мною должностных обязанностей по Трудовому договору, заключенному между мною и МБОУСОШ №4, предусматривающих работу с персональным данным мне будет предоставлен доступ к указанной информации.

Настоящим добровольно принимаю на себя обязательства:

не передавать (в любом виде) и не разглашать третьим лицам и работникам МБОУСОШ №4 не имеющим на это право в силу выполняемых ими должностных обязанностей или в соответствии с решением руководителя МБОУСОШ №4, информацию, содержащую персональные данные (за исключением собственных данных), которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей;

в случае попытки третьих лиц или работников МБОУСОШ №4, не имеющих на это право, получить от меня информацию, содержащую персональные данные работников МБОУСОШ №4, немедленно сообщать об этом факте своему непосредственному или (в случае отсутствия непосредственного) вышестоящему руководителю;

не использовать информацию, содержащую персональные данные работников МБОУСОШ №4, с целью получения выгоды;

выполнять требования закона и иных нормативных правовых актов Российской Федерации, а так же внутренних документов МБОУСОШ №4, регламентирующих вопросы защиты интересов субъектов персональных данных, порядка обработки и защиты персональных данных;

в течение 3 (Трех) лет после прекращения моих прав на допуск к информации, содержащей персональные данные работников МБОУСОШ №4 (переход на должность, не предусматривающую доступ к персональным данным работников МБОУСОШ №4 или прекращения Трудового договора), не разглашать и не передавать третьим лицам и неуполномоченным на это работникам МБОУСОШ №4, известную мне информацию, содержащую персональные данные.

Я ознакомлен (а) с положениями законодательства Российской Федерации, а так же внутренними организационно-распорядительными документами, в части защиты персональных данных.

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с действующим законодательством Российской Федерации.

\_\_\_\_\_/\_\_\_\_\_ «\_\_\_» \_\_\_\_\_ г.

(фамилия, инициалы)

(подпись)

ПЛАН

внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБОУСОШ №4 на 2016-2017 уч. год

Мероприятие	Периодичность регулярных мероприятий	Периодичность плановых мероприятий	Исполнитель
Контроль соблюдения правил доступа к ПДн	Еженедельно	1 раз в четверть	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Кузьминов
Контроль соблюдения режима защиты	Еженедельно	1 раз в четверть	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Кузьминов
Контроль выполнения антивирусной политики	Еженедельно	1 раз в четверть	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Кузьминов
Контроль выполнения парольной политики	Еженедельно	1 раз в четверть	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Кузьминов
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	1 раз в четверть	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Кузьминов
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн		1 раз в четверть	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Кузьминов
Контроль обновления ПО и единообразия применяемого ПО	Еженедельно	1 раз в четверть	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Кузьминов
Контроль обеспечения резервного копирования		1 раз в четверть	Ответственный за обеспечение безопасности персональных данных информационных систем

			персональных данных Кузьминов
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз		1 раз в четверть	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Кузьминов
Поддержание в актуальном состоянии нормативно-организационных документов		1 раз в четверть	Ответственный за организацию обработки ПДн Кузьминов

**ПОЛИТИКА  
В ОБЛАСТИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ  
ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ  
ПЕРСОНАЛЬНЫХ ДАННЫХ МБОУ СОШ № 4**

**ВВЕДЕНИЕ**

Настоящий документ «Политика в отношении обработки персональных данных» (далее - Политика) определяет высокоуровневую политику в отношении обработки МБОУ СОШ № 4 персональных данных субъектов и содержит сведения о реализуемых требованиях к защите персональных данных в МБОУ СОШ № 4.

Настоящая Политика разработана на основе действующих правовых и нормативных документов по защите конфиденциальной информации и персональных данных.

Под персональными данными в настоящем документе понимается любая информация, относящаяся к прямо или косвенно, определенному или определяемому физическому лицу (субъекту персональных данных).

4. Настоящая Политика утверждается приказом руководителя МБОУ СОШ № 4 и подлежит пересмотру по мере необходимости.

**1. Общие положения**

Согласно Статье Федерального закона от 25.07.2006 г. № 152-ФЗ МБОУ СОШ № 4 как оператор персональных данных обязан опубликовать, или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

МБОУ СОШ № 4 в рамках выполнения своей деятельности осуществляет обработку персональных данных и, в соответствии с действующим законодательством Российской Федерации, является оператором персональных данных с соответствующими правами и обязанностями, определенными Федеральным законом № 152 от 27.07.2006 г. «О персональных данных» и иными нормативными правовыми актами Российской Федерации (далее - РФ). Состав обрабатываемых данных, категории субъектов, чьи персональные данные обрабатываются МБОУ СОШ № 4, цели и правовые основания их обработки закреплены для каждой информационной системы МБОУ СОШ № 4 «Перечнем персональных данных, обрабатываемых в ИСПДН».

С целью поддержания деловой репутации и обеспечения выполнения законодательных требований МБОУ СОШ № 4 считает для себя обязательным обеспечение соответствия обработки персональных данных требованиям законодательства РФ в области защиты информации и персональных данных, и требует аналогичных мер от третьих лиц, которым передаются и (или) могут передаваться персональные данные на основании п.3 Постановления Правительства Российской Федерации от 01 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

**1. Принципы, правила и цели обработки персональных данных**

Обработка персональных данных осуществляется МБОУ СОШ № 4 с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»:

- обработка персональных данных осуществляется на законной и справедливой основе;

- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки;
- обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечивает точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- МБОУ СОШ № 4 принимает необходимые меры по удалению или уточнению неполных или неточных данных;
- хранение персональных данных в МБОУ СОШ № 4 осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, к примеру Федеральный Закон от 22.10.2004 г. №125-ФЗ «Об архивном деле в Российской Федерации» или договором, стороной которого является субъект персональных данных;
- обрабатываемые персональные данные уничтожаются или обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством РФ;

Обработка персональных данных осуществляется МБОУ СОШ № 4 только в случаях:

- наличия согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством РФ;
- наличия заключенного договора, по которому МБОУ СОШ № 4 обязуется осуществлять обработку персональных данных субъектов по поручению оператора;
- необходимости достижения целей, предусмотренных нормативно-правовыми актами Российской Федерации и трудовым законодательством, для осуществления и выполнения возложенных законодательством РФ на МБОУ СОШ № 4 функций, полномочий и обязанностей;
- необходимости осуществления прав и законных интересов МБОУ СОШ № 4 или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
  - когда персональные данные открыты для неограниченного круга лиц, доступ к которым предоставлен субъектом персональных данных либо по его просьбе;
- обязательного раскрытия и подлежащих к опубликованию персональных данных в соответствии с законодательством РФ;
- организации пропускного режима на территории МБОУ СОШ № 4.

Согласно требованиям Федерального закона № 152 от 27.07.2006 г. «О персональных данных», МБОУ СОШ № 4 в установленном порядке прошел регистрацию как оператор персональных данных. В открытом и общедоступном реестре операторов персональных данных, размещенном на официальном сайте Роскомнадзора как уполномоченного лица по защите прав и свобод субъектов персональных данных, содержится следующая актуальная информация:

- адрес МБОУ СОШ № 4;
- цели обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;

- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых МБОУ СОШ № 4 способов обработки персональных данных;
- фамилия, имя, отчество физического лица, ответственного в МБОУ СОШ № 4 за организацию обработки персональных данных, и номера его контактных телефонов, почтовые адреса и адреса электронной почты;
- описание мер, которые МБОУ СОШ № 4 обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии трансграничной передачи персональных данных в процессе их обработки.

МБОУ СОШ № 4 обязуется не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ и договором с субъектом.

МБОУ СОШ № 4 не обрабатывает специальные и биометрические категории персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведения, характеризующие биологические и физические особенности человека. (данный абзац необходимо рассматривать субъективно для каждой информационной системы персональных данных оператора.)

МБОУ СОШ № 4 не осуществляет трансграничную передачу персональных данных субъектов персональных данных.

МБОУ СОШ № 4 не принимает решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных.

## 2. Меры, направленные на обеспечение выполнения МБОУ СОШ № 4 обязанностей, предусмотренных законодательством РФ.

МБОУ СОШ № 4 осуществляет следующие организационно-технические меры для защиты персональных данных:

- назначение МБОУ СОШ № 4 лица, ответственного за организацию обработки персональных данных;
- издание документов, определяющих политику МБОУ СОШ № 4 в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона № 152 «О персональных данных», включая:
  - определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ № 4
  - применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ № 4, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных;
  - применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;



- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем персональных данных МБОУ СОШ № 4 - учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных МБОУ СОШ № 4, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных МБОУ СОШ № 4;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных МБОУ СОШ № 4
- осуществление внутреннего контроля соответствия обработки персональных данных законодательству РФ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике МБОУ СОШ № 4 в отношении обработки персональных данных, локальным актам МБОУ СОШ № 4;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства РФ, соотношение указанного вреда и принимаемых МБОУ СОШ № 4 мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством РФ;
- ознакомление работников МБОУ СОШ № 4, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику МБОУ СОШ № 4 в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.
- доступ к содержанию электронного журнала сообщений возможен исключительно для администратора безопасности, или лица, ответственного за обеспечение безопасности персональных данных в информационных системах МБОУ СОШ № 4.

#### 4. Право субъекта персональных данных на доступ к его персональным данным

4.1. Субъект персональных данных имеет право на получение сведений, указанных в части 6 настоящего раздела, за исключением случаев, предусмотренных законодательством РФ. Субъект персональных данных вправе требовать от законных представителей МБОУ СОШ № 4 уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4.2. Сведения, указанные в части 6 настоящего раздела, предоставляются законными представителями МБОУ СОШ № 4 субъекту персональных данных в доступной форме.

4.3. Сведения, указанные в части 6 настоящего раздела, предоставляются субъекту персональных данных или его представителю законными представителями МБОУ СОШ № 4 при получении запроса субъекта персональных данных или его представителя в письменной форме.

4.4. В случае, если сведения, указанные в части 6 настоящего раздела, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к законным представителям МБОУ СОШ № 4 или направить МБОУ СОШ № 4 повторный запрос в письменной форме в целях получения сведений, указанных в части 6 настоящего раздела, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса.

4.5. Субъект персональных данных вправе обратиться повторно к законному представителю МБОУ СОШ № 4 или направить повторный письменный запрос в МБОУ СОШ № 4 в целях получения сведений, указанных в части 6 настоящего раздела, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 настоящего раздела, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

4.6. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных МБОУ СОШ № 4;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые МБОУ СОШ № 4 способы обработки персональных данных;
- 4) наименование и место нахождения МБОУ СОШ № 4, сведения о лицах (за исключением работников образовательного учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с МБОУ СОШ № 4 или на основании законодательства РФ;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных законодательством РФ;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению МБОУ СОШ № 4, если обработка поручена или будет поручена такому лицу.

## ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ МБОУ СОШ № 4 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила работы с обезличенными персональными данными МБОУ СОШ № 4 разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящие Правила определяют порядок работы с обезличенными данными МБОУ СОШ № 4. Настоящие Правила утверждаются директором МБОУ СОШ № 4 и действуют постоянно.

### УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ.

1.3. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных МБОУ СОШ № 4 и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

1.4. Способы обезличивания при условии дальнейшей обработки персональных данных:

- 1.4.1. уменьшение перечня обрабатываемых сведений;
- 1.4.2. замена части сведений идентификаторами;
- 1.4.3. обобщение – понижение точности некоторых сведений;

1.4.4. понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);

1.4.5. деление сведений на части и обработка в разных информационных системах;

1.4.6. другие способы.

1.5. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

1.6. Для обезличивания персональных данных годятся любые способы явно не запрещенные законодательно.

1.7. Перечень должностей работников МБОУ СОШ № 4 ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, приведен в п.4 настоящих Правил;

1.7.1. Руководитель МБОУ СОШ № 4 принимает решение о необходимости обезличивания персональных данных;

1.7.2. Лица, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания, если это необходимо;

1.7.3. Лица, обслуживающие базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

#### **ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ**

1.8. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

1.9. Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

1.10. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

1.10.1. парольной политики;

1.10.2. антивирусной политики;

1.10.3. правил работы со съемными носителями (если они используются);

1.10.4. правил резервного копирования;

1.10.5. правил доступа в помещения, где расположены элементы информационных систем;

1.10.6. иных предусмотренных законодательством РФ законов и правовых актов.

1.11. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

1.11.1. правил хранения бумажных носителей;

1.11.2. правил доступа к ним и в помещения, где они хранятся;

1.11.3. иных предусмотренных законодательством РФ законов и правовых актов.

#### **ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ МБОУ СОШ № 4 ОТВЕТСТВЕННЫХ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ОБЕЗЛИЧИВАНИЮ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

1. Директор
2. Заместители директора
3. Секретарь школы
4. Социальный педагог
5. Психологи
6. Педагоги
7. Классные руководители

**Регламент осуществления внутреннего контроля за обеспечением уровня защищенности персональных данных и соблюдения условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в информационных системах персональных данных МБОУ СОШ № 4**

**1. Общие положения**

Настоящий Регламент осуществления внутреннего контроля за обеспечением уровня защищенности персональных данных и соблюдения условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в информационных системах персональных данных (далее – Регламент) устанавливает и определяет единый и обязательный порядок проведения контрольных мероприятий для каждой из подсистем, входящих в систему защиты персональных данных информационных систем персональных данных (далее - ИСПДн ) МБОУ СОШ № 4.

Настоящий Регламент утверждается и вводится руководителем МБОУ СОШ № 4. и является обязательным для исполнения.

**2. Порядок подготовки к проведению контрольных мероприятий**

Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдения условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн МБОУ СОШ № 4.

проводятся в следующих целях:

проверка выполнения требований организационно-распорядительной документации образовательного МБОУ СОШ № 4.

- действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

оценка уровня осведомленности и знаний работников МБОУ СОШ № 4.

- в области обработки и защиты персональных данных (далее - ПДн);
- оценка обоснованности и эффективности применяемых мер и средств защиты.

**Виды контрольных мероприятий**

Контрольные мероприятия подразделяются на внутренние и внешние. Внутренние контрольные мероприятия осуществляются силами работников МБОУ СОШ № 4.

Ответственных за обеспечение безопасности ПДн. При проведении внешних контрольных мероприятий привлекаются сторонние организации.

Кроме того, контрольные мероприятия подразделяются на плановые и внеплановые.

Плановые контрольные мероприятия проводятся периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее - План) и направлены на постоянное совершенствование системы защиты персональных данных МБОУ СОШ № 4.

Внеплановые контрольные мероприятия проводятся на основании решения инженера по безопасности группы информационных технологий. Решение о проведении внеплановых контрольных мероприятий может быть принято в следующих случаях:

- по результатам расследования инцидента информационной безопасности;
- по результатам внешних контрольных мероприятий, проводимых регулирующими органами.

Кроме того любой работник МБОУ СОШ № 4 вправе подготавливать обоснованные предложения о необходимости проведения внеплановых контрольных мероприятий и предоставить их лицу, ответственному за обеспечение безопасности ПДн.

### **План проведения контрольных мероприятий**

Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

План проведения внутренних контрольных мероприятий (как плановых, так и внеплановых) включает следующие сведения по каждому из мероприятий:

- цели проведения контрольных мероприятий;
- задачи проведения контрольных мероприятий,
- объекты контроля (процессы, подразделения, информационные системы и т.п.);
- состав участников, привлекаемых для проведения контрольных мероприятий;
- сроки и этапы проведения контрольных мероприятий.

Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий (см. раздел ).

### **Оформление результатов проведенных контрольных мероприятий**

По итогам проведения внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает отчет, в котором указывается:

- описание проведенных мероприятий по каждому из этапов в соответствии с планом;
- отклонения от плана, в случае их наличия;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений.
- заключение по итогам проведения внутреннего контрольного мероприятия.

Отчет передается на рассмотрение руководству МБОУ СОШ № 4.

Общая информация о проведенном контрольном мероприятии фиксируется в Журнале учета мероприятий по обеспечению и контролю безопасности ПДн, обрабатываемых в ИСПДн МБОУ СОШ № 4. (см. Приложение 1 настоящего Регламента).

## **3. Общий порядок проведения контрольных мероприятий**

Контрольные мероприятия проводятся при обязательном участии лица, ответственного за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы информационных систем, администраторы информационной безопасности.

Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех работников, у которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

### **3.1. Контрольные мероприятия в подсистеме управления доступом**

При проведении контрольных мероприятий могут выполняться следующие проверки:

- проверка соответствия установленных прав доступа (в прикладных системах, базах данных и т.п.) полномочиям в рамках трудовых обязанностей работника;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;

- проверка процесса идентификации, аутентификации и авторизации при входе пользователя в систему (обращении к информационным ресурсам информационных систем);
- проверка механизмов блокирования доступа к средствам защиты от несанкционированного доступа<sup>1</sup> (далее - НСД) при выполнении устанавливаемого числа неудачных попыток ввода пароля;
- проверка системы смены пароля принудительным образом (по истечению срока действия пароля);
- проверка выполнения требований по стойкости пароля.

### **3.2. Контрольные мероприятия в подсистеме регистрации и учета**

При проведении контрольных мероприятий в подсистеме регистрации и учета, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка системных журналов на наличие зарегистрированных попыток несанкционированного доступа;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации и внутренних документах компании;
- имитация попытки несанкционированного доступа в систему, для проверки работы системы регистрации попытки НСД в системном журнале;
- проверка способов защиты системного журнала регистрации от уничтожения или модификации нарушителем<sup>2</sup>;
- проверка функционирующей системы автоматического непрерывного мониторинга событий в системе, которые могут являться причиной реализации угроз (создание, редактирование, запись, компиляция объектов).

Кроме того, при проведении проверок в части учета и хранения носителей персональных данных могут выполняться следующие проверки:

- проверка мест хранения носителей ПДн, сейфов и металлических шкафов, надежность их замков;
- проверка выполнения установленного порядка учета и хранения носителей ПДн;
- проверка фактического наличия всех носителей ПДн, в том числе учетные журналы, дела, документы (поступившие, изданные, переведенные на выделенное хранение);
- проверка фактического наличия всех носителей ПДн, переданных на архивное хранение;
- проверка фактического наличия всех не подшитых в дела и поступивших документов, содержащих ПДн, независимо от даты их регистрации;
- проверка номенклатуры дел с целью выделения документов, содержащих ПДн, для передачи в архив или на уничтожение;
- проверка правильности проставления регистрационных данных носителей, документов и дел, и учетных журналов;
- проверка правильности проставления в журнале отметок о движении носителей.

### **3.3. Контрольные мероприятия в подсистеме обеспечения целостности**

При проведении контрольных мероприятий в подсистеме обеспечения целостности, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка механизмов контроля целостности пакетов обновлений средств защиты информации с использованием контрольных сумм;

---

<sup>1</sup> Несанкционированный доступ - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационной системой

<sup>2</sup> Нарушитель (субъект атаки) – лицо (или иницируемый им процесс), проводящее (проводящий) атаку.

- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка целостности используемого программного обеспечения, путем вычисления контрольных сумм;
- проверка фактического наличия экземпляров резервных копий;
- проверка целостности сделанных резервных копий путем восстановления данных;
- имитация выполнения резервного копирования и восстановления данных при аварийном режиме функционирования системы.

### **3.4. Контрольные мероприятия в подсистеме антивирусной защиты**

При проведении контрольных мероприятий в подсистеме антивирусной защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка рабочих станций и серверов станций на наличие установленных программных средств антивирусной защиты;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка механизма своевременного обновления программных средств антивирусной защиты (в т.ч. баз данных вирусных сигнатур) на всех рабочих и серверных станциях;
- запуск полного сканирования системы в режиме реального времени антивирусным средством;
- проверка антивирусным средством используемых отчуждаемых носителей;
- проверка функционирования механизмов принудительной проверки используемых съемных носителей;
- имитация попыток заражения вредоносным программным обеспечением<sup>3</sup> серверных и рабочих станций;
- просмотр системных журналов и отчетов на наличие зафиксированных случаев заражения вредоносным ПО.

### **3.5. Контрольные мероприятия в подсистеме обеспечения безопасного межсетевого взаимодействия**

При проведении контрольных мероприятий в подсистеме обеспечения безопасного межсетевого взаимодействия, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия установленных межсетевых экранов требуемому уровню защищенности;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- имитация попыток проникновения в «закрытый» сегмент сети из открытого, в том числе с применением специального ПО;
- проверка системных журналов на наличие зафиксированных попыток обращения к «закрытым» ресурсам.

### **3.6. Контрольные мероприятия в подсистеме анализа защищенности**

При проведении контрольных мероприятий в подсистеме анализа защищенности, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка выполнения своевременного обновления ПО, используемого для анализа защищенности, в т.ч. баз данных уязвимостей;

---

<sup>3</sup> Вредоносное программное обеспечение - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных

- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- имитация попыток преодоления системы защиты, проверка системных журналов на наличие зафиксированных попыток НСД.

### **3.7. Контрольные мероприятия в подсистеме обнаружения и предотвращения вторжений**

При проведении контрольных мероприятий в подсистеме обнаружения и предотвращения вторжений, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации.

### **3.8. Контрольные мероприятия в подсистеме защиты от утечек по техническим каналам**

При проведении контрольных мероприятий в подсистеме защиты от утечек по техническим каналам, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка в помещениях, где ведется обработка ПДн,;
- проверка размещения дисплеев рабочих станций, серверов и демонстрационного оборудования (проекторы, телевизоры и т.п.) таким образом, чтобы исключалась возможность просмотра посторонними лицами текстовой и графической информации, содержащей персональные данные.

### **3.9. Контрольные мероприятия в подсистеме физической защиты**

При проведении контрольных мероприятий в подсистеме физической защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка введения журналов учета посетителей, проходящих на территорию МБОУ СОШ № 4.
- проверка введения журналов посетителей, проходящих в защищаемые помещения;
- проверка электронных журналов СКУД на предмет попыток НСД в защищаемые помещения сотрудников, не имеющих права доступа в данные помещения;
- проверка наличия ключей (в том числе и электронных пропусков) от защищаемых помещений, а так же проверка сохранности вторых экземпляров ключей от защищаемых помещений;
- просмотр всех заявлений об утерянных ключах (в том числе и электронных пропусках) по которым можно получить доступ в защищаемые помещения, а так же проверка принятых мер (блокирование электронного пропуска, смена замка);
- проверка надежности замков, установленных в защищаемых помещениях;
- имитация попытки проникновения в защищаемые помещения для проверки срабатывания сигнализации и (или) системы контроля и управления доступом.

### **3.10. Контрольные мероприятия в подсистеме криптографической защиты**

При проведении контрольных мероприятий в подсистеме криптографической защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации.
- проверка сохранности эксплуатационной и технической документации и ключевых документов на средства криптографической защиты;
- проверка журналов учета средств криптографической защиты и используемых криптоключей на правильность их ведения и хранения;
- проверка знаний работниками, использующими средства криптографической защиты, правил применения этих средств и правил обращения с криптоключами;
- проверка функционирования средств криптографической защиты путем имитации процессов, шифрования и дешифрования информации.





									е рек оме нда	нару шен ий
	• 2	• 3	• 4	• 5	• 6	• 7	• 8	• 9	• 10	

•

- Приложение №9
- к приказу МБОУ СОШ №4
- от 12.08.2016 года № 348

• Положение  
«О порядке уничтожения персональных данных»

• 1. Общие положения

• 1.1. Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в МБОУСОШ №4 № 4 г. , в целях реализации: Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства Российской Федерации от 21.03.2012 № 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.

• 2. Порядок уничтожения информации, содержащей персональные данные,

- при достижении целей обработки или при наступлении иных законных оснований

• 2.1. Уничтожение документов, содержащих ПД, производится:

- - по достижении целей их обработки согласно номенклатуре дел и документов;
- - по достижении окончания срока хранения ПД, оговоренного в соответствующем соглашении заинтересованных сторон; в том числе, если они не подлежат архивному хранению.

• 2.2. Уничтожение документов, содержащих персональные данные, производится в случае выявления неправомерной обработки персональных данных в срок, не превышающий десяти рабочих дней с момента выявления неправомерной обработки персональных данных.

• 2.3. Уничтожение информации с ПД, хранящейся в электронном виде на материальных носителях, производится путем выполнения процедуры специальной подготовки материальных носителей (многократное форматирование разделов, выделенных под хранение данных).

• 2.4. Уничтожение материальных носителей с ПД осуществляется механическим либо электромагнитным воздействием с помощью специализированных средств (шредер, уничтожитель оптических дисков и т.п.). Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

• 2.5. Уничтожение производится по мере необходимости, в зависимости от объемов накопленных для уничтожения документов.

• 2.6. Для уничтожения материальных носителей и информации на материальных носителях документально создается экспертная комиссия в составе не менее 2 человек. Уничтожение осуществляется по акту. Уничтожение документов производится в присутствии всех членов комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (состав комиссии утверждается приказом). После уничтожения материальных носителей членами комиссии подписывается акт в трех экземплярах (Приложение 1) делается запись в журналах их учета и регистрации, а также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №\_\_ (дата)».

• 2.7. Накапливаемые для уничтожения документы, копии документов, черновики, содержащие персональные данные, должны храниться отдельно.

•

•

• Акт № \_\_\_\_\_

• об уничтожении носителей, содержащих персональные данные

• Комиссия в составе:

• Председатель – \_\_\_\_\_

• Члены комиссии – \_\_\_\_\_

• провела отбор бумажных, электронных, магнитных и оптических носителей персональных данных и другой конфиденциальной информации (далее носители) и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежит гарантированному уничтожению и составила настоящий акт о том, что произведено уничтожение носителей персональных данных в составе:

• № • п/п	• Дата	• Т	• Уч • етн • ый • но • ме • р • но • сит • еля	• Категория • информации	• Примеча • ние
•	•	•	•	•	•

• Всего носителей \_\_\_\_\_  
(цифрами и прописью количество)

• На указанных носителях персональные данные уничтожены путем

• \_\_\_\_\_  
(стирания на устройстве гарантированного уничтожения информации и т.п.)

• Перечисленные носители ПД уничтожены путем

• \_\_\_\_\_  
(разрезания/сжигания/размагничивания/физического уничтожения/ механического уничтожения / иного способа)

• Председатель комиссии: \_\_\_\_\_ / \_\_\_\_\_ /

• Члены комиссии: \_\_\_\_\_ / \_\_\_\_\_ /

• \_\_\_\_\_ / \_\_\_\_\_ /

- Приложение №2
- к Порядку уничтожения персональных данных при достижении целей их обработки

- Типовая форма журнала уничтожения носителей персональных данных

- Журнал уничтожения носителей персональных данных

- Журнал начат \_\_\_\_\_
- Журнал завершен \_\_\_\_\_
- Ответственный \_\_\_\_\_ (Ф.И.О.)  
  - На \_\_\_\_\_ листах

	<ul style="list-style-type: none"> <li>• Наименование ИСП</li> <li>• Дн, в которой уничтожаются персональные данные</li> </ul>	<ul style="list-style-type: none"> <li>• Ф.И.О. субъекта, персдаанные которого по дл</li> </ul>	<ul style="list-style-type: none"> <li>• Обоснование уничтожения</li> </ul>	<ul style="list-style-type: none"> <li>• Наименование файла, его местоположения</li> </ul>	<ul style="list-style-type: none"> <li>• Дата уничтожения</li> </ul>	<ul style="list-style-type: none"> <li>• Ф.И.О. и подпись Исполнителя</li> </ul>	<ul style="list-style-type: none"> <li>• Ф.И.О. и подпись ответственного лица за обработку персональных данных</li> </ul>
--	--	---	---	--	--	--	---

		еж ац ие ун ич то же ни ю					НБХ
	• 2	• 3	• 4	• 5	• 6	• 7	• 8

•  
•