

Согласовано
Советом ОУ
Протокол №2
от «03» ноября 2016 г.

Принято
Педагогическим советом
Протокол №7
от «03» ноября 2016 г.

Утверждаю
Директор МБОУ «Солгин-
ская СШ №86»
Кулагина А.Н.
Приказ №501
от «07» ноября 2016 г.



**Положение
о защите персональных данных в МБОУ «Солгинская СШ № 86»
с использованием средств автоматической защиты
и без автоматической защиты**

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Конституцией РФ, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федеральным законом «Об образовании», Постановлением правительства Российской Федерации от 17.11.2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федеральным законом «Об образовании», Постановлением правительства Российской Федерации от 17.11.2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящее Положение определяет порядок обработки персональных данных работников, учащихся и родителей (законных представителей) МБОУ «Солгинская СШ № 86» (далее Школа) и гарантии конфиденциальности сведений, предоставляемых администрации.

1.3. Персональные данные сотрудников, учащихся, родителей (законных представителей) являются конфиденциальной информацией.

**2. Понятие и состав персональных данных сотрудников,
учащихся, родителей (законных представителей)**

2.1. Персональные данные сотрудника – это необходимая работодателю в связи с трудовыми отношениями информация о конкретном сотруднике.

К персональным данным сотрудника относятся:

- 1) фамилия, имя, отчество;
- 2) год, месяц, дата и место рождения, а также иные данные, содержащиеся в удостоверении личности сотрудника;
- 3) данные о семейном, социальном и имущественном положении;
- 4) данные об образовании сотрудника, наличии специальных знаний или подготовки;
- 5) данные о профессии, специальности сотрудника;
- 6) сведения о доходах сотрудника;
- 7) данные медицинского характера, в случаях, предусмотренных законодательством;
- 8) данные о членах семьи сотрудника;
- 9) данные о месте жительства, почтовый адрес, телефон сотрудника, а также членов его семьи;
- 10) данные, содержащиеся в трудовой книжке сотрудника и его личном деле, страховом свидетельстве государственного пенсионного страхования, свидетельстве о постановке на налоговый учет;
- 11) данные, содержащиеся в документах воинского учета (при их наличии);
- 12) иные персональные данные, при определении объема и содержания которых работодатель руководствуется настоящим Положением и законодательством РФ.

2.1.1. В состав персональных данных учащихся Школы входят документы, содержащие информацию о паспортных данных, свидетельства о рождении, медицинского страхового полиса, отношении к воинской обязанности, месте жительства, телефонов, состоянии здоровья, личных достижений, социальное положение, а также о предыдущих местах их учебы.

2.1.2. В состав персональных данных родителей (законных представителей) учащихся Школы входят документы, содержащие информацию о паспортных данных, образовании, семейном положении, наличии детей, месте жительства, телефонов, социальное положение, а также о месте их работы.

2.1.3. В состав персональных данных соискателей на вакантные должности Школы входят документы, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, наличии детей, месте жительства, состоянии здоровья, личных профессиональных достижений, социальное положение, а также о предыдущих местах их работы.

3. Обработка персональных данных

3.1. Обработка персональных данных сотрудника, учащегося, родителя (законного представителя) – получение, хранение, комбинирование, передача или любое другое использование персональных данных сотрудника. Обработка персональных данных сотрудника учащегося, родителя (законного представителя) осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов, содействия работнику в трудоустройстве, обучении, продвижении по службе, обеспечения личной безопасности сотрудника, учащегося, родителя (законного представителя), контроля качества и количества выполняемой работы и обеспечения сохранности имущества, оплаты труда, пользования льготами, предусмотренными законодательством РФ и актами работодателя.

3.2. Работодатель не имеет права получать и обрабатывать персональные данные сотрудника, учащегося, родителя (законного представителя), о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни сотрудника только с его письменного согласия.

Работодатель не имеет права получать и обрабатывать персональные данные сотрудника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

При принятии решений, затрагивающих интересы сотрудника, работодатель не имеет права основываться на персональных данных сотрудника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.3. На основании норм Трудового кодекса РФ (ст. 86), а также исходя из положений п. 2 ст. 6 Федерального закона №152-ФЗ "О персональных данных", обработка персональных данных осуществляется работодателем без письменного согласия сотрудника, за исключением случаев, предусмотренных федеральным законом.

3.4. Все персональные данные о работнике работодатель может и должен получить от него самого.

3.5. Работник обязан предоставлять работодателю достоверные сведения о себе и своевременно сообщать ему об изменении своих персональных данных. Работодатель имеет право проверять достоверность сведений, предоставленных работником, сверяя данные, предоставленные работником, с имеющимися у сотрудника документами.

3.6. В случаях, когда работодатель может получить необходимые персональные данные сотрудника только у третьего лица, работодатель должен уведомить об этом сотрудника и получить от него письменное согласие по установленной форме.

Работодатель обязан сообщить работнику о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа сотрудника дать письменное согласие на их получение.

3.7. Персональные данные сотрудника хранятся в Школе в личном деле сотрудника. Личные дела хранятся в бумажном виде в папках и находятся в сейфе или в несгораемом шкафу.

Персональные данные сотрудника в Школе хранятся также в электронном виде. Доступ к электронным базам данных, содержащим персональные данные работников, обеспечиваются системой паролей.

Персональные данные учащегося, родителя (законного представителя) хранятся в Школе в личном деле учащегося. Личные дела хранятся в бумажном виде в приемной кабинета директора.

Примечание: Хранение персональных данных работников в бухгалтерии и иных структурных подразделениях работодателя, сотрудники которых имеют право доступа к персональным данным, осуществляется в порядке исключаяющем к ним доступ третьих лиц.

3.8. Сотрудник работодателя, имеющий доступ к персональным данным в связи с исполнением трудовых обязанностей обеспечивает хранение информации, содержащей персональные данные сотрудника, учащегося, родителя (законного представителя) исключаяющее доступ к ним третьих лиц.

В отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные (соблюдение "политики чистых столов").

При уходе в отпуск, служебной командировке и иных случаях длительного отсутствия сотрудника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные лицу, на которое локальным актом Школы (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей.

Примечание: В случае, если такое лицо не назначено, то документы и иные носители, содержащие персональные данные, передаются другому сотруднику, имеющему доступ к персональным данным по указанию директора Школы.

При увольнении сотрудника, имеющего доступ к персональным данным, документы и иные носители, содержащие персональные данные, передаются другому сотруднику, имеющему доступ к персональным данным по указанию директора Школы.

3.9. Доступ к персональным данным имеют сотрудники, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей согласно перечню должностей (Положение о персональных данных работников, соискателей на вакантные должности, учащихся и их родителей (законных представителей) МБОУ «СОЛГИНСКАЯ СШ № 86»)

В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией директора, доступ к персональным данным сотрудника может быть предоставлен иному работнику, должность которого не включена в Перечень должностей сотрудников, имеющих доступ к персональным данным, и которым они необходимы в связи с исполнением трудовых обязанностей.

3.10. В случае если Школе оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным, то соответствующие данные предоставляются только после подписания с ними соглашения о неразглашении конфиденциальной информации.

В исключительных случаях, исходя из договорных отношений с контрагентом, допускается наличие в договорах пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных.

3.11. Процедура оформления доступа к персональным данным сотрудника включает в себя:

- ознакомление сотрудника под роспись с настоящим Положением. Примечание: При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных сотрудника, с данными актами также производится ознакомление сотрудника под роспись.
- истребование с сотрудника (за исключением директора Школы) письменного обязательства о соблюдении конфиденциальности персональных данных сотрудника и соблюдении правил их обработки, подготовленного по установленной форме.

3.12. Сотрудники Школы, имеющие доступ к персональным данным, имеют право получать только те персональные данные сотрудника, учащегося, родителя (законного представителя) которые необходимы им для выполнения конкретных трудовых функций.

3.13. Доступ к персональным данным без специального разрешения имеют работники, занимающие в Школе следующие должности:

- директор;
- заместители директора;
- специалист по кадрам;
- инженер ИВТ;
- главный бухгалтер

3.14. Допуск к персональным данным сотрудника других сотрудников Школы, не имеющих надлежащим образом оформленного доступа, запрещается.

3.15. Работник имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи (за исключением случаев предусмотренных федеральным законом), содержащей его персональные данные. Работник имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

3.16. Работодатель вправе передавать персональные данные сотрудника в бухгалтерию и иные структурные подразделения, в случае необходимости исполнения сотрудниками соответствующих структурных подразделений своих трудовых обязанностей.

При передаче персональных данных сотрудника, специалисты по кадровой работе предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и истребуют от этих лиц письменное обязательство в соответствии с п. 3.11. настоящего Положения.

3.17. Передача (обмен и т.д.) персональных данных внутри Школы осуществляется только между сотрудниками, имеющими доступ к персональным данным работников.

3.18. Передача персональных данных третьим лицам осуществляется только с письменного согласия сотрудника, которое должно включать в себя:

- фамилию, имя, отчество, адрес сотрудника, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес работодателя, получающего согласие сотрудника;
- цель передачи персональных данных;
- перечень персональных данных, на передачу которых дает согласие работник;
- срок, в течение которого действует согласие, а также порядок его отзыва.

Примечание: Согласия сотрудника на передачу его персональных данных третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника; когда третьи лица оказывают услуги работодателю на основании заключенных договоров, а также в случаях, установленных федеральным законом и настоящим Положением.

3.19. Не допускается передача персональных данных сотрудника учащегося, родителя (законного представителя) в коммерческих целях без его письменного согласия.

3.20. Сотрудники Школы, передающие персональные данные третьим лицам, должны передавать их с обязательным составлением акта приема-передачи документов (иных материальных носителей), содержащих персональные данные работников. Акт составляется по установленной форме, и должен содержать следующие условия:

- уведомление лица, получающего данные документы об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена;
- предупреждение об ответственности за незаконное использование данной
- конфиденциальной информации в соответствии с федеральными законами.

Передача документов (иных материальных носителей), содержащих персональные данные осуществляется при наличии у лица, уполномоченного на их получение:

- договора на оказание услуг Организации;
- соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе, предусматривающих защиту персональных данных сотрудника;
- письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные сотрудника, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных несет работник, осуществляющий передачу персональных данных сотрудника третьим лицам.

3.21. Представителю сотрудника (в том числе адвокату) персональные данные передаются в порядке, установленном действующим законодательством и настоящим Положением. Информация передается при наличии одного из документов:

- нотариально удостоверенной доверенности представителя сотрудника;

- письменного заявления сотрудника, написанного в присутствии сотрудника отдела кадров работодателя (если заявление написано работником не в присутствии сотрудника отдела кадров, то оно должно быть нотариально заверено).

Доверенности и заявления хранятся в отделе кадров в личном деле сотрудника.

3.22. Предоставление персональных данных государственным органам производится в соответствии с требованиями действующего законодательства и настоящим Положением.

3.23. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника, за исключением случаев, когда передача персональных данных сотрудника без его согласия допускается действующим законодательством РФ.

3.24. Документы, содержащие персональные данные, могут быть отправлены через организацию федеральной почтовой связи. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие персональные данные вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее, конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

4. Организация защиты персональных данных

4.1. Защита персональных данных от неправомерного их использования или утраты обеспечивается директором.

4.2. Общую организацию защиты персональных данных осуществляет специалист по кадрам.

4.3. Специалист по кадрам обеспечивает:

- ознакомление сотрудника под роспись с настоящим Положением. При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных сотрудника, с данными актами также производится ознакомление сотрудника под роспись.

- истребование с сотрудников (за исключением лиц, указанных в пункте 3.13 настоящего Положения) письменного обязательства о соблюдении конфиденциальности персональных данных сотрудника и соблюдении правил их обработки;

- общий контроль за соблюдением сотрудниками работодателя мер по защите персональных данных сотрудника.

4.4. Организацию и контроль за защитой персональных данных работников структурных подразделениях работодателя, сотрудники которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

4.5. Защите подлежат:

- информация о персональных данных;
- документы, содержащие персональные данные;
- персональные данные, содержащиеся на электронных носителях.

4.6. Защита сведений, хранящихся в электронных базах данных работодателя, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается разграничением прав доступа с использованием учетной записи и системой паролей.

5. Заключительные положения

5.1. Иные права, обязанности, действия сотрудников, в трудовые обязанности которых входит обработка персональных данных, определяются также должностными инструкциями.

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

5.3. Разглашение персональных данных сотрудника, учащегося или родителя (законного представителя) (передача их посторонним лицам, в том числе, сотрудникам Школы, не имеющим

к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные сотрудника, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативными актами (приказами, распоряжениями) Школы, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарного взыскания – замечания, выговора, увольнения.

5.4. Сотрудники, имеющие доступ к персональным данным и совершившие указанный дисциплинарный проступок, несут полную материальную ответственность в случае причинения его действиями ущерба работодателю (п.7 ст. 243 Трудового кодекса РФ).

5.5. Сотрудники, имеющие доступ к персональным данным, виновные в незаконном разглашении или использовании персональных данных работников, учащихся или родителей (законных представителей) без их согласия из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со ст. 183 Уголовного кодекса РФ.

**Перечень
сведений конфиденциального характера
в МБОУ «Солгинская СШ № 86»**

В настоящем Перечне предусматриваются категории сведений, представляющих конфиденциальную информацию (персональные данные) в МБОУ «Солгинская СШ № 86», разглашение которых может нанести материальный, моральный или иной ущерб интересам данного учреждения, его работникам и учащимся.

№ п/п	Перечень сведений	Срок действия
1	Финансы	
1.1	Сведения о бухгалтерском учете (за исключением годового баланса).	3 года
1.2	Сведения о финансовых операциях.	3 года
1.3	Сведения о величине доходов и расходов, о состоянии дебиторской и кредиторской задолженностях (за исключением годового баланса).	3 года
1.4	Сведения, содержащиеся в финансово - договорных схемах Организации.	+ 1 год после окончания действия договора
2	Личная безопасность сотрудников	
2.1	Персональные данные, сведения о фактах, событиях и обстоятельствах частной жизни сотрудника.	постоянно
2.2	Сведения об используемой в коллективе системе стимулов, укрепляющих дисциплину, повышающих производительность труда.	На период действия
2.3	Информация о личных отношениях специалистов как между собой, так и с руководством, сведения о возможных противоречиях, конфликтах внутри коллектива.	3 года
3	Персональные данные об обучающихся	
3.1	Персональные данные обучающегося.	постоянно
3.2	Персональные данные родителей (законных представителей).	постоянно
3.3	Сведения, необходимые для предоставления обучающемуся гарантий и компенсаций, установленных действующим законодательством.	постоянно
4	Персональные данные о детях, оставшихся без попечения родителей	
4.1	Персональные данные детей, оставшихся без попечения родителей.	постоянно
4.2	Персональные данные кандидатов в усыновители, приемные родители, опекуны.	постоянно
5	Безопасность	
5.1	Сведения о порядке и состоянии защиты конфиденциальной информации.	постоянно
5.2	Сведения о защищаемых информационных ресурсах в локальных сетях Организации.	постоянно
5.2	Сведения об охране организации, пропускном и внутриобъектовом режиме, системе сигнализации, о наличии средств контроля и управления доступом.	постоянно

ИНСТРУКЦИЯ
пользователя по обеспечению информационной безопасности
автоматизированного рабочего места, выделенного для обработки
конфиденциальной информации (персональных данных)
в МБОУ «Солгинская СШ № 86»

В Инструкции пользователя по обеспечению информационной безопасности при работе с базами данных школы (далее – Инструкция пользователя) использованы следующие термины и определения:

1. База данных (далее - БД) - централизованное хранилище информации, оптимизированное для многопользовательского доступа и работающее под управлением системы управления базами данных (далее - СУБД).
2. Комплекс программных средств (далее - КПС) - система или приложение, использующее непосредственный доступ к БД.
3. Идентификатор (учетное имя или login) - присвоенная пользователю индивидуально буквенно-числовая последовательность, используемая для идентификации пользователя при установлении доступа к БД и позволяющая однозначно определять работу конкретного пользователя в БД.
4. Пароль - секретная персональная последовательность символов, известная только пользователю, которая используется совместно с идентификатором для доступа в БД и позволяет подтвердить, что доступ к БД осуществляет именно конкретный пользователь.
5. Пользователи - должностные лица МБОУ «Солгинская СШ № 86», а также все другие лица и организации, работающие с БД школы.
6. Администратор БД - должностное лицо МБОУ «Солгинская СШ № 86», уполномоченные для выполнения административных функций и обеспечивающие функционирование БД и ее безопасность соответственно.
7. Локально-вычислительная сеть (далее - ЛВС) - группа компьютеров, а также периферийное оборудование, объединенные одним или несколькими автономными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.
8. Политика информационной безопасности - комплекс организационно-технических мероприятий, правил и условий использования информационных систем МБОУ «Солгинская СШ № 86», определяющих нормальное функционирование систем и обеспечение безопасности информации, обрабатываемой в МБОУ «Солгинская СШ № 86»

Настоящий документ разработан на основе Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, с целью совершенствования методического обеспечения деятельности в данной области государственных и муниципальных органов, юридических и физических лиц, организующих и (или) осуществляющих обработку персональных данных (ПД), определяющих цели и содержание обработки ПД (операторов), а также заказчиков и разработчиков информационных систем персональных данных (ИСПД) при решении ими задач по обеспечению безопасности ПД.

Общие положения по организации доступа
к конфиденциальной информации в МБОУ «Солгинская СШ № 86»

1. Инструкция пользователя определяет комплекс организационно - технических мероприятий по обеспечению безопасности конфиденциальной информации, хранящейся на компьютерах школы в БД и обрабатываемой с помощью средств вычислительной техники в МБОУ «Солгинская СШ № 86».
2. Инструкция пользователя является частью политики информационной безопасности МБОУ «Солгинская СШ № 86», предназначена для обеспечения эффективной организации и управления доступом пользователей к конфиденциальной информации, хранящейся на компьютерах школы и в БД МБОУ «Солгинская СШ № 86», и содержит требования по обеспечению ин-

формационной безопасности учреждения в части выполнения операций со конфиденциальной информацией и по организации и управлению доступом к БД.

3. Требования Инструкции пользователя обязательны для выполнения всеми пользователями, которым предоставляется доступ к конфиденциальной информации МБОУ «Солгинская СШ № 86».

4. Доступ к конфиденциальной информации МБОУ «СОЛГИНСКАЯ СШ № 86» предоставляется исключительно пользователям, утверждённым приказом администрации школы через предоставленный системным администратором школы пароль.

5. Решение задач, связанных с организацией и управлением доступом должностных лиц школы к конфиденциальной информации, осуществляется системным администратором школы.

При возникновении ситуаций, не включенных в положения настоящей Инструкции пользователя, решение принимает системный администратор.

6. Для доступа к БД школы у каждого пользователя БД должен иметь свой уникальный идентификатор и пароль доступа к БД.

7. Доступ к БД школы может быть предоставлен с любого компьютера административной локальной сети.

8. Доступ к БД предоставляется пользователям на срок действия их трудовых отношений и исполнения служебных обязанностей в МБОУ «СОЛГИНСКАЯ СШ № 86».

Обязанности и ответственность пользователей автоматизированных рабочих мест, выделенных для обработки конфиденциальной информации.

1. Перед началом первой работы с конфиденциальной информацией пользователь обязан изучить Инструкцию пользователя и ознакомиться с ответственностью за выполнение требований Инструкции пользователя при работе с конфиденциальной информацией под роспись.

2. Пользователю запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа к конфиденциальной информации другим лицам. Запрещается хранение пароля в общедоступных местах, позволяющих другим лицам получить информацию о пароле.

3. Пользователь конфиденциальной информации обязан обеспечивать правильность ввода и коррекции данных, за которые он отвечает.

4. Пользователь обязан закрывать соединение с БД школы на время своего отсутствия у рабочей станции БД или вообще выходить по доступу к ресурсам компьютера с конфиденциальными данными из своего идентификатора (*например, teacher, secret, adminic и т.п., через Пуск_Завершить сеанс Имя идентификатора*).

5. В случае выявления инцидентов с доступом к ресурсам компьютера с конфиденциальными данными (фактов несанкционированного доступа посторонними людьми, людьми без допуска к конфиденциальным данным) пользователь обязан незамедлительно сообщить об этом системному администратору школы.

6. В случае выявления инцидентов с доступом к БД школы (фактов несанкционированного доступа к БД, блокировки доступа, утери или компрометации пароля и т.п.) пользователь обязан незамедлительно сообщить об этом администратору БД.

7. Установку и конфигурирование программного обеспечения на компьютерах с доступом к конфиденциальным данным школы выполняет системный администратор или администратор БД школы. Пользователям данных рабочих мест запрещается самостоятельно устанавливать какое-либо программное обеспечение.

8. Пользователю запрещается использовать информацию, полученную в результате доступа к конфиденциальным данным школы, в целях, не предусмотренных его функциональными обязанностями и технологическими схемами. Он не вправе разглашать, использовать в личных целях, либо передавать третьим лицам, в том числе государственным органам, конфиденциальную информацию, за исключением случаев, установленных законами Российской Федерации.

9. При нарушениях правил, связанных с информационной безопасностью, пользователь несет ответственность, установленную действующим законодательством Российской Федерации.

10. Пользователь несет ответственность за все действия, совершенные от имени его идентификатора, учетной записи или логина, если не доказан факт несанкционированного использования таковых.