

Государственное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа №35 с углубленным изучением английского языка
Василеостровского района Санкт-Петербурга

ПРИНЯТО

на заседании Педагогического совета
ГБОУ СОШ №35
от 04.06 2019 г. №5

Председатель _____
(О.А. Кусок)

УТВЕРЖДАЮ



директор
ГБОУ СОШ №35

О.А. Кусок

Приказ № 56/2 от 04.06.2019 г.

УЧТЕНО

Мнение Совета родителей
ГБОУ СОШ №35

Протокол №5 от 03.06.2019 _____

УЧТЕНО

Мнение Совета обучающихся
ГБОУ СОШ №35

Протокол №5 от 03.06.2019 _____

ПРАВИЛА
обработки персональных данных
в государственном бюджетном общеобразовательном учреждении средней
общеобразовательной школы №35 с углубленным изучением английского языка
Василеостровского района Санкт-Петербурга

1. Общие положения

1.1. Настоящие Правила обработки персональных данных (далее по тексту - Правила) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных в государственном бюджетном общеобразовательном учреждении средней общеобразовательной школы №35 с углубленным изучением английского языка Василеостровского района Санкт-Петербурга (далее по тексту - Образовательное учреждение).

1.2. Настоящие Правила являются обязательными для исполнения всеми сотрудниками Образовательного учреждения, имеющих доступ к персональным данным и осуществляющих обработку персональных данных.

1.3. Организация деятельности по обработке персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации. Нормативной основой для организации деятельности по обработке персональных данных являются:

- Федеральный закон РФ от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями и дополнениями);
- Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями и дополнениями);
- Федеральный закон РФ от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (с изменениями и дополнениями);
- Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи» (с изменениями и дополнениями);
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Распоряжение Правительства Российской Федерации от 17.12.2009 № 1993-р «Об утверждении сводного перечня первоочередных государственных и муниципальных услуг, предоставляемых органами исполнительной власти субъектов Российской Федерации и органами местного самоуправления в электронном виде, а также услуг, предоставляемых в электронном виде учреждениями субъектов Российской Федерации и муниципальными учреждениями» (с изменениями и дополнениями);
- Приказ Министерства образования и науки РФ от 30.08.2013 № 1015 «Об утверждении Порядка организации и осуществления образовательной деятельности по основным общеобразовательным программам - образовательным программам начального общего, основного общего и среднего общего образования» (с изменениями и дополнениями);
- Приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (с изменениями и дополнениями);
- Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями);
- Письмо Министерства образования и науки РФ от 15.02.2012 № АП-147/07 «О методических рекомендациях по внедрению систем ведения журналов успеваемости в электронном виде» (с изменениями и дополнениями);

- Письмо Министерства образования и науки РФ от 21.10.2014 № АК-3358/08 «Об уточнениях в методические рекомендации по внедрению систем ведения журналов успеваемости в электронном виде»;
- «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях. СанПиН 2.4.2.2821-10» (с изменениями и дополнениями);
- Закон Санкт-Петербурга от 17.07.2013 № 461-83 «Об образовании в Санкт-Петербурге» (с изменениями и дополнениями);
- Распоряжение Комитета по образованию от 31.10.2011 № 2299-р «Об утверждении регламента по предоставлению услуги по предоставлению информации о текущей успеваемости учащегося, ведения электронного дневника и электронного журнала учащегося» (с изменениями и дополнениями);
- иные нормативно-правовые акты органов управления образованием различного уровня;
- Устав Образовательного учреждения;
- настоящие Правила;
- приказы и распоряжения директора Образовательного учреждения.

1.4. В настоящих Правилах используются следующие понятия:

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), включая любую информацию, относящуюся к сотруднику, обучающемуся, родителям (законным представителям) обучающихся, в том числе, его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

2. Правила обработки Персональных данных

2.1. Обработка персональных данных в Образовательном учреждении должна осуществляться на законной основе.

2.2. Обработка персональных данных в Образовательном учреждении должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Цели обработки персональных данных в обязательном порядке указываются непосредственно в письменном согласии на обработку персональных данных, даваемом субъектом персональных данных или его законным представителем.

2.3. Письменное согласие на обработку персональных данных должно быть получено Образовательным учреждением от субъекта персональных данных или его законного представителя до начала непосредственной обработки персональных данных.

При оформлении согласия на обработку персональных данных субъект персональных данных или его законный представитель ставится в известность о возможном отзыве согласия на обработку персональных данных; при получении отзыва согласия на обработку персональных данных в Образовательном учреждении прекращается последующая обработка персональных данных, производимая на основании ранее полученного согласия.

2.4. Конкретные сроки обработки персональных данных указываются в согласии на обработку персональных данных, даваемом субъектом персональных данных или его законным представителем.

Сроки хранения материальных носителей, содержащих сведения о персональных данных, устанавливаются в соответствии с требованиями действующего законодательства.

2.5. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

2.6. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

2.7. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

2.8. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

Ответственный за осуществление обработки персональных данных в Образовательном учреждении, должен принимать необходимые меры по удалению или уточнению неполных или неточных персональных данных.

2.9. Мерами, направленными на выявление и предотвращение нарушений, предусмотренных законодательством, являются:

1) осуществление внутреннего контроля соответствия обработки персональных данных нормам Федерального закона № 152-ФЗ «О персональных данных» (далее по тексту -Федеральный закон) и принятыми в соответствии с ним нормативными правовыми актами;

2) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых Образовательным учреждением мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

3) ознакомление работников Образовательного учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных.

2.10. Обеспечение безопасности персональных данных достигается:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных

данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) проведением в установленном порядке процедуры оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер по их недопущению;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

2.11. Целью обработки персональных данных в Образовательном учреждении является обеспечение соблюдения законов и иных нормативных правовых актов.

2.12. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъект персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен Федеральным законом или договором, стороной которого является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

2.13. В случае выявления неправомерной обработки персональных данных, осуществляемой работником, в срок, не превышающий три рабочих дня с даты этого выявления, работник обязан прекратить неправомерную обработку персональных данных.

В случае если обеспечить правомерность обработки персональных данных невозможно, работник, осуществляющий обработку персональных данных, в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных работник обязан уведомить субъекта персональных данных или его представителя, а в случае если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

2.14. В случае достижения целей обработки персональных данных работник обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между Образовательным учреждением и субъектом персональных данных, либо если Образовательное учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных, на основаниях, предусмотренных Федеральным законом или другими федеральными законами.

2.15. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных работник обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий три рабочих дня с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Образовательным учреждением и субъектом персональных данных.

Об уничтожении персональных данных государственный работник обязан уведомить субъекта персональных данных не позднее трех рабочих дней со дня уничтожения.

2.16. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, работник осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок, не превышающий шесть месяцев, если иной срок не установлен федеральными законами.

3. Порядок обработки Персональных данных в информационных системах персональных данных с использованием средств автоматизации

3.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

3.2. Мероприятия безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.3. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации.

4. Порядок обработки персональных данных без использования средств автоматизации

4.1. Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка персональных данных) в соответствии с постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации.

4.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

4.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

4.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4.5. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних носителях информации.

4.6. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

4.7. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

4.8. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

4.9. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

5. Заключительные положения

5.1. Настоящие Правила принимаются решением Педагогического совета Образовательного учреждения с учетом мнения совета обучающихся, с учетом мнения совета родителей (законных представителей) несовершеннолетних обучающихся (при наличии указанных советов) и утверждаются приказом директора Образовательного учреждения.

5.2. Изменения и дополнения в настоящие Правила (в том числе, в виде новой редакции Правил) принимаются решением Педагогического совета Образовательного учреждения с учетом мнения совета обучающихся, с учетом мнения совета родителей (законных представителей) несовершеннолетних обучающихся (при наличии указанных советов) и утверждаются приказом директора Образовательного учреждения.