УТВЕРЖДАЮ

Директор ГБОУ СО «Школа-интернат АОП с. Ш. Буерак»

_____ /Пушкова И.В./

Приказ № 23-2 от 01.03.2021

Подписано цифровой подписью: Пушкова И.В.
DN: cn=Пушкова И.В., o=ГБОУ СО "Школа-интернат АОП с. Широкий Буерак", ou, email=skola-internatSB@yandex.ru, c=RU
Дата: 2021.07.01 13:56:10 +04'00'

Политика
обработки персональных данных
ГБОУ СО «Школа-интернат АОП с. Широкий Буерак»

1. Общие положения

1.1. Настоящая Политика по обработке персональных данных (далее – Политика):

- является основополагающим внутренним документом ГБОУ СО «Школа-интернат АОП с. Широкий Буерак» (далее - Учреждение), регулирующим вопросы обработки персональных данных;

– разработана в целях обеспечения соответствия с законодательством Российской Федерации обработки, хранения и защиты ИСПДн единого окна цифровой обратной связи (далее – ПОС);

– раскрывает основные категории персональных данных, обрабатываемых Учреждением, цели, способы и принципы обработки персональных данных, права и обязанности работников при обработке персональных данных, права субъектов персональных данных, а также перечень мер, применяемых в целях обеспечения безопасности персональных данных при их обработке;

– предназначена для работников Учреждения, осуществляющих обработку персональных данных в целях непосредственной реализации ими закрепленных в Политике принципов, а также является информационным ресурсом для субъектов персональных данных, позволяющим определить концептуальные основы деятельности Учреждения при обработке персональных данных.

2. Источники нормативного правового регулирования вопросов обработки персональных данных

2.1. Политика Учреждения в области обработки персональных данных определяется на основании следующих нормативных правовых актов РФ:

1. Конституция Российской Федерации;
2. Федеральный закон РФ от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3. Федеральный закон РФ от 27.07.2006 г. №152-ФЗ «О персональных данных»;
4. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».
5. ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;
6. ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
7. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»;
8. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации»;
9. РД 50-680-88. Методические указания. Автоматизированные системы. Основные положения;

10. РД 50-34.698-90. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов;

11. РД Гостехкомиссии России. «Положение об обязательной сертификации продукции по требованиям безопасности информации» 1994 г.;

12. РД Гостехкомиссии России. «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» 1992 г.;

13. РД Гостехкомиссии России. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» 1992 г.;

14. РД Гостехкомиссии России. «Защита от несанкционированного доступа к информации. Термины и определения» 1992 г.;

15. РД Гостехкомиссии России. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» 1997 г.;

16. РД Гостехкомиссии России. «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1999 г.;

17. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Государственной технической комиссией при Президенте РФ 25.11.1994 г.;

18. Требования к защите персональных данных при их обработке в информационных системах персональных данных, утверждены Постановлением Правительства Российской Федерации №1119 от 01.11.2012 г.;

19. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждены приказом ФСТЭК России №21 от 18.02.2013 г.;

20. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСБ России с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством РФ требований к защите персональных данных для каждого из уровней защищенности, утверждены приказом ФСБ России №378 от 10.07.2014 г.;

2.2. Во исполнение настоящей Политики в Учреждении приказами утверждаются следующие локальные нормативные правовые акты:

- Инструкция администратора информационных систем персональных данных (ИС);
- Инструкция пользователя информационных систем персональных данных;
- Инструкция по действиям пользователей информационных систем персональных данных в нештатных ситуациях;
- Инструкция по организации антивирусной защиты информационных систем персональных данных;
- Инструкция по порядку проведения проверок состояния защиты персональных данных;
- План внутренних проверок состояния защиты персональных данных;
- Перечень обрабатываемых персональных данных;
- План мероприятий по защите персональных данных;
- Порядок организации и проведения работ по обработке и защите персональных данных Учреждения;
- Акт определения уровня защищенности ПОС;
- Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в информационных системах.

и иные локальные документы, принимаемые во исполнение требований, действующих нормативных правовых актов РФ в области обработки персональных данных.

3. Основные термины и понятия, используемые в локальных документах Учреждения, принимаемых по вопросу обработки персональных данных

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации, Перечнем ПДн, обрабатываемых в Учреждении и локальными актами Учреждения.

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

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

Предоставление персональных данных – действия, направленные на раскрытие ПДн определенному кругу.

Использование персональных данных – действия (операции) с ПДн, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц.

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

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

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

Информационная система персональных данных – информационная система, представляющая собой совокупность содержащихся в базе данных ПДн и их обработку, информационных технологий и технических средств.

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

Общедоступные персональные данные – ПДн, доступ неограниченного круга лиц, к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Трансграничная передача персональных данных – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

4. Общие условия обработки персональных данных

4.1 Обработка ПОС в Учреждении осуществляется на основе следующих принципов:

4.1.1 Законности и справедливости обработки ПДн.

4.1.2 Законности целей и способов обработки ПДн и добросовестности.

4.1.3 Соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Учреждения.

4.1.4 Соответствия содержания и объема обрабатываемых ПДн целям обработки ПДн.

4.1.5 Достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн.

4.1.6 Недопустимости объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.1.7 Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

4.1.8 Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

4.1.9 Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.1.10 Субъект ПДн является собственником своих ПДн и самостоятельно решает вопрос передачи Учреждению своих ПДн.

4.1.11 Держателем ПОС является Учреждение, которому субъект ПДн передает во владение свои ПДн. Учреждение выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

4.1.12 Комплекс мер по защите ПДн направлен на предупреждение нарушений доступности, целостности и конфиденциальности ПДн.

4.1.13 Учреждение при обработке ПДн обязано принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий, в соответствии с требованиями к обеспечению безопасности ПДн при их обработке в ИС.

4.1.14 Мероприятия по защите ПДн определяются Положением, приказами, инструкциями и другими внутренними документами Учреждения.

4.2 Для защиты ПДн применяются следующие принципы и правила:

4.2.1 Ограничение и регламентация состава работников, функциональные обязанности которых требуют доступа к информации, содержащей ПДн.

4.2.2 Строгое избирательное и обоснованное распределение документов и информации между работниками.

4.2.3 Рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации.

4.2.4 Знание работниками требований нормативно-методических документов по защите ПДн.

4.2.5 Распределение персональной ответственности между работниками, участвующими в обработке ПДн, за выполнение требований по обеспечению безопасности ПДн.

4.2.6 Установление режима конфиденциальности в соответствии с требованиями по обеспечению безопасности ПДн при работе с конфиденциальными документами и базами данных.

4.2.7 Определение угроз безопасности персональных данных при их обработке в информационных системах.

4.2.8 Исключение бесконтрольного пребывания посторонних лиц в помещениях, в которых ведется обработка ПДн и находится соответствующая вычислительная техника.

4.2.9 Организация порядка уничтожения персональных данных.

4.2.10 Своевременное выявление нарушений требований разрешительной системы доступа.

4.2.11 Воспитательная и разъяснительная работа с работниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

4.2.12 Регулярное обучение работников по вопросам, связанным с обеспечением безопасности ПДн.

4.2.13 Ограничение доступа к техническим средствам и системам обработки информации, на которых содержатся ПДн.

4.2.14 Создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

4.2.15 Резервирование защищаемых данных (создание резервных копий).

4.3 Целью обработки персональных данных является исполнение п.3 перечня поручений Президента Российской Федерации от 1 марта 2020 года Пр-354, Постановления Правительства Российской Федерации «О проведении эксперимента по использованию федеральной государственной информационной системы «Единый портал государственных муниципальных услуг (функций)».

4.4 Правовое основание обработки персональных данных:

- Федеральный закон 27 июля 2020 года № 210 «Об организации предоставления государственных и муниципальных услуг»;
- Постановление правительства РФ № 451 от 08.06.2011 г. «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».