УПРАВЛЕНИЕ ОБРАЗОВАНИЯ
АДМИНИСТРАЦИИ СЕРГИЕВО-ПОСАДСКОГО МУНИЦИПАЛЬНОГО РАЙОНА МОСКОВСКОЙ ОБЛАСТИ
Муниципальное бюджетное учреждение дополнительного образования
Детская школа искусств имени Елены Дмитриевны Поленовой (г.Хотьково)
МБУДОДШИ им. Е.Д.Поленовой (г.Хотьково)
141370, г. Хотьково, ул. 2-я Рабочая, д.27а, тел. 54-3-59-09, факс 54-3-59-09
E-mail: a35948@yandex.ru

«Утверждаю»
Директор МБУДОДШИ
им.Е.Д.Поленовой (г.Хотьково)
_____ Е.М. Вороная
Приказ от 30.10.2018 №71

ПОЛИТИКА
обработки и защиты персональных данных в муниципальном бюджетном учреждении дополнительного образования Детская школа искусств имени Елены Дмитриевны Поленовой (г.Хотьково)

1.Общие положения

1.1. Настоящая Политика определяет порядок обработки и защиты персональных данных в муниципальном бюджетном учреждении дополнительного образования Детская школа искусств имени Елены Дмитриевны Поленовой (г.Хотьково) Сергиево-Посадского муниципального района Московской области (далее – Учреждение) с целью защиты прав и свобод человека, и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Политика обработки персональных данных в Учреждении разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, п.2ст 18.1 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.01.2001 №» 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", Положение по обработке и защите персональных данных в муниципальном бюджетном учреждении дополнительного образования Детская школа искусств имени Елены Дмитриевны Поленовой (г.Хотьково), утвержденного приказам от 30.10.2018 № 71 и иными нормативными правовыми актами, действующими на территории Российской Федерации.

1.2.1. Основные понятия и определения используемые в Политике:

«персональные данные» - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

«оператор» - муниципальный орган, организующий и (или) осуществляющий обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

«субъект» - субъект персональных данных (далее- ПДн);

«обработка персональных данных» - действия (операции) с ПДн, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

«распространение персональных данных» - действия, направленные на передачу ПДн определенному кругу лиц (передача ПДн) или на ознакомление с ПДн неограниченного круга лиц;

«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 сбора, систематизации, накопления, использования, распространения ПДн, в том числе их передачи;

«уничтожение персональных данных» - действия, в результате которых невозможно восстановить содержание ПДн в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

«обезличивание персональных данных» - действия, в результате которых невозможно определить принадлежность ПДн конкретному субъекту ПДн;

«информационная система персональных данных» (далее - ИСПДн) - информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств;

«конфиденциальность персональных данных» - обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания;

«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;

«информация» - сведения (сообщения, данные) независимо от формы их представления;

«доступ к информации» - возможность получения информации и ее использования;

«документированная информация» - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

1.3. Действие Политики распространяется на все персональные данные субъектов, обрабатываемые в информационных системах персональных данных управления образования с применением средств автоматизации и без применения таких средств.

2. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Принципы и условия обработки персональных данных

- Учреждение, как собственник информационных ресурсов;
- сотрудники Учреждения;
- обучающиеся Учреждения;
- граждане, обращающиеся в Учреждение по вопросам, относящимся к компетенции Учреждения.

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- своевременного доступа к необходимым им персональным данным (их доступности);
- достоверности (полноты, точности, адекватности, целостности) персональных данных;
- конфиденциальности (сохранения в тайне) персональных данных;
- защиты от навязывания им ложных (недостоверных, искаженных) персональных данных;
- разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с персональными данными;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи персональных данных;
- защиты персональных данных от незаконного распространения.

2.2. Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений учреждения от

возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств персональных данных:

- доступности персональных данных для легальных пользователей (устойчивого функционирования информационных систем Учреждения, при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);

- целостности и аутентичности (подтверждение авторства) персональных данных, хранимых и обрабатываемых в информационных системах Учреждения и передаваемой по каналам связи;

- конфиденциальности - сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

2.3. Основные задачи системы обеспечения безопасности персональных данных

Для достижения основной цели защиты и обеспечения указанных свойств персональных данных система обеспечения информационной безопасности Учреждения должна обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем Учреждения;

- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

- защиту от вмешательства в процесс функционирования информационных систем Учреждения посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Учреждения (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;

- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

- защиту от несанкционированной модификации используемых в информационных системах Учреждения программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

- защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

2.4. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите ресурсов информационных систем Учреждения (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

- журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационных систем;

- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Учреждения по вопросам обеспечения безопасности информации;

- назначением должностных лиц в Учреждении, ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки, а также контроль за их деятельностью в данном направлении;

- наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Учреждения;

- четким знанием и строгим соблюдением всеми пользователями информационных систем Учреждения требований организационно - распорядительных документов по вопросам обеспечения безопасности информации;

- персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Учреждения;

- непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Учреждения;

- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

- эффективным контролем над соблюдением пользователями информационных ресурсов Учреждения требований по обеспечению безопасности информации;

- юридической защитой интересов Учреждения при взаимодействии с внешними организациями (связанном с обменом персональными данными) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

3. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Построение системы обеспечения безопасности персональных данных Учреждения, и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

3.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности персональных данных Учреждением в соответствии с действующим законодательством в области защиты персональных данных, а также других законодательных актов по безопасности информации РФ, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с персональными данными. Принятые меры безопасности персональных данных не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях. Все пользователи информационных систем Учреждения должны иметь представление об ответственности за правонарушения в области обработки персональных данных.

3.2. Системность

Системный подход к построению системы защиты информации в Учреждении предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем Учреждения, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников). Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

3.3. Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

3.4. Непрерывность защиты

Обеспечение безопасности персональных данных - процесс, осуществляемый руководством Учреждения, и сотрудниками всех уровней. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности Учреждения.

3.5. Своевременность

Постановку задач по комплексной защите персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных систем в целом и их систем защиты.

Разработка системы защиты ведется параллельно с разработкой и развитием самой защищаемой информационной системы.

3.6. Преемственность и совершенствование

Постоянное совершенствование мер и средств защиты персональных данных на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем Учреждения и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите.

3.7. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности персональных данных ценности информационных ресурсов и возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

3.8. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

3.9. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к персональным данным предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

3.10. Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Учреждением своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры Учреждения;
- изменение существующих или внедрение принципиально новых информационных систем;
- новые технические средства.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

4. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

4.1. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности информационных систем Учреждения подразделяются на:

- правовые (законодательные);
- организационные (административные);
- физические;
- технические (аппаратурные и программные).

4.2. Регламентация доступа в помещения

Компоненты информационных систем Учреждения размещены в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, АРМ и т. п.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

Во время обработки персональных данных в помещениях должен присутствовать только персонал, допущенный к работе с персональными данными.

Запрещается прием посетителей в помещениях, когда осуществляется обработка персональных данных.

По окончании рабочего дня, помещения, в которых размещаются компоненты информационных систем Учреждения, запираются на ключ. Здание Учреждения охраняется частным охранным предприятием.

4.3. Регламентация допуска сотрудников к использованию информационных ресурсов

В рамках разрешительной системы (матрицы) доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационными системами Учреждения и доступ к ее ресурсам строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

- каждый сотрудник пользуется только предписанными ему правами по отношению к персональным данным, с которыми ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с ответственным по безопасности информационных систем персональных данных;

Все сотрудники Учреждения и обслуживающий персонал, несут персональную ответственность за нарушения установленного порядка обработки персональных данных, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению персональных данных Учреждения.

Обработка персональных данных в компонентах информационных систем Учреждения должна производиться в соответствии с утвержденными инструкциями.

4.4. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

В целях поддержания режима информационной безопасности аппаратно - программная конфигурация автоматизированных рабочих мест сотрудников Учреждения, с которых возможен доступ к ресурсам информационных систем, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

В компонентах информационных систем и на рабочих местах пользователей устанавливаться и использоваться лицензионные программные средства.

4.5. Средства обеспечения безопасности персональных данных

Для обеспечения информационной безопасности Учреждения используются следующие средства защиты:

- физические средства;
- технические средства;
- средства идентификации и аутентификации пользователей;

- средства разграничения доступа;
- средства обеспечения и контроля целостности;
- средства оперативного контроля и регистрации событий безопасности.

Средства защиты применяются ко всем ресурсам информационных систем Учреждения, независимо от их вида и формы представления информации в них.

4.6. Контроль эффективности системы защиты

Контроль эффективности защиты персональных данных осуществляется с целью своевременного выявления и предотвращения утечки персональных данных за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение персональных данных, разрушение средств информатизации. Контроль может проводиться привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты персональных данных проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

5. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

При достижении целей обработки персональных данных, записи в базах данных уничтожаются по акту.

6. ИЗМЕНЕНИЕ ПОЛИТИКИ

Учреждение имеет право вносить изменения в настоящую Политику. Новая редакция Политики вступает в силу с момента ее утверждения и размещения в общедоступном месте, если иное не предусмотрено новой редакцией Политики.

7. ОБРАТНАЯ СВЯЗЬ

Муниципальное бюджетное учреждение дополнительного образования Детская школа искусств имени Елены Дмитриевны Поленовой (г.Хотьково) Сергиево-Посадского муниципального района Московской области, юридический/фактический адрес: Московская область, Сергиево-Посадский муниципальный район, г. Хотьково, ул.2-я Рабочая, д.27а,
ИНН: 5042070009, ОГРН: 1035008357174