

**ПРИНЯТО:**

Общим собранием  
работников МДОАУ № 174  
протокол № 3 от 10.03 2023

**УТВЕРЖДЕНО**

приказом МДОАУ № 174  
от 10.03.2023 № 100  
заведующий МДОАУ № 174  
Лукиных Т.А.

**ПОЛИТИКА  
информационной безопасности  
муниципального дошкольного образовательного  
автономного учреждения  
«Детский сад № 174»**

## **Введение**

Настоящая Политика информационной безопасности (далее – Политика) МДОАУ «Детский сад №174» (далее – ДОУ) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона №266-ФЗ от 14.07.2022 «О внесении изменений в Федеральный закон «О персональных данных», постановления Правительства Российской Федерации от 11 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», «Положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного директором ФСТЭК от 05.01.2010 г. № 58. В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности ИСПДн ДОУ.

### **1. Общие положения**

Целью настоящей Политики является обеспечение безопасности объектов защиты ДОУ от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Политика информационной безопасности утверждается руководителем ДОУ и вводится в действие приказом заведующего ДОУ.

### **2. Область действия**

Требования настоящей Политики распространяются на всех сотрудников ДОУ (штатных, временных, работающих по договору и т.п.), а также на всех прочих лиц.

Настоящая Политика действует в отношении всей информации, которую ДОУ может получить о пользователе во время использования им любых сервисов и служб Сайта ДОУ (далее – Сервисы).

Согласие пользователя на предоставление персональной информации, данное им в соответствии с настоящей Политикой в рамках использования одного из Сервисов, распространяется на все Сервисы Сайта.

### **3. Требования к персоналу по обеспечению защиты ПДн**

Все сотрудники ДОУ, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятыми процедурами работы с элементами ИСПДн и СЗПДн.

Сотрудники ДОУ, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать к ним, а также возможность их утери или использования третьими лицами.

Пользователи несут персональную ответственность за сохранность идентификаторов. Сотрудники ДОО должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники ДОО должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами ДОО, третьим лицам. При работе с ПДн в ИСПДн сотрудники ДОО обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов. Сотрудники ДОО должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за обработку ПДн.

#### **4. Цели сбора и обработки персональной информации пользователей сайта ДОО**

ДОО собирает и хранит только те персональные данные, которые необходимы для оказания услуг пользователю сайта.

Персональная информация пользователя может использоваться в следующих целях: Идентификация стороны в рамках использования Сервисов Сайта. Связь с пользователем в случае необходимости, в том числе направление уведомлений, запросов и информации, связанных с оказанием услуг, а также обработка запросов и заявок от пользователя. Улучшение качества услуг. Проведение статистических и иных исследований на основе обезличенных данных.

ДОО не проверяет достоверность персональной информации, предоставляемой пользователями сайта, и не осуществляет контроль за их дееспособностью. Однако ДОО исходит из того, что пользователь предоставляет достоверную и достаточную персональную информацию по вопросам, предлагаемым в форме регистрации, и поддерживает эту информацию в актуальном состоянии.

#### **5. Условия обработки персональной информации пользователя и её передачи третьим лицам**

ДОО хранит персональную информацию пользователей в соответствии с внутренним регламентом. В отношении персональной информации пользователя сохраняется ее конфиденциальность, кроме случаев добровольного предоставления пользователем информации о себе для общего доступа всем пользователям Сайта.

ДОО вправе передать персональную информацию пользователя третьим лицам в следующих случаях: Пользователь явно выразил свое согласие на такие действия. Передача необходима в рамках использования пользователем определенного Сервиса либо для оказания услуги пользователю. При этом обеспечивается конфиденциальность персональной информации, а пользователь будет явным образом уведомлен о такой передаче. Передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

## **6. Изменение пользователем Сайта персональной информации**

6.1. Пользователь может в любой момент изменить (обновить, дополнить) или удалить предоставленную им персональную информацию или её часть, направив соответствующее заявление по почтовому адресу ДООУ.

## **7. Меры, применяемые для защиты персональной информации пользователей**

ДООУ принимает все необходимые меры для защиты любых персональных данных, предоставляемых пользователями.

Доступ к персональным данным имеют только уполномоченные сотрудники ДООУ, уполномоченные сотрудники сторонних компаний (т.е. поставщиков услуг) или наших деловых партнеров, подписавшие договор о конфиденциальности и защите персональных данных.

Все сотрудники ДООУ, имеющие доступ к персональным данным, должны придерживаться политики по обеспечению конфиденциальности и защиты персональных данных.

В целях обеспечения конфиденциальности информации и защиты персональных данных ДООУ поддерживает соответствующую ИТ-среду и принимает все меры, необходимые для предотвращения несанкционированного доступа (хакерства).

## **8. Изменение Политики конфиденциальности. Применимое законодательство**

ДООУ имеет право вносить изменения в настоящую Политику конфиденциальности.

При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее размещения, если иное не предусмотрено новой редакцией Политики.

К настоящей Политике и отношениям между пользователем и ДООУ, возникающим в связи с применением Политики обработки персональных данных, подлежит применению действующее законодательство Российской Федерации.