

**МУНИЦИПАЛЬНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ДЕТСКИЙ САД № 180 СОВЕТСКОГО РАЙОНА ВОЛГОГРАДА»
(ДОУ ДЕТСКИЙ САД № 180)**

СОГЛАСОВАНО
Советом Детского сада
(Протокол от 31.08.2018 г. № 3)

УТВЕРЖДЕН
приказом МОУ Детского сада № 180
от 31.08.2018 г. № 116-О
Заведующий ДОУ Детского сада № 180
Е.А. Зверева



**Политика информационной безопасности
в муниципальном дошкольном образовательном учреждении
«Детский сад № 180 Советского района Волгограда»**

1. Общие положения

- 1.1. Настоящая Политика информационной безопасности (далее — Политика) в муниципальном дошкольном образовательном учреждении «Детский сад № 180 Советского района Волгограда» (далее — ДОУ) разработана в соответствии с Федеральным законом от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных».
- 1.2. Настоящая Политика определяет задачи, функции, обязанности, ответственность и права ответственных за информационную безопасность.
- 1.3. Ответственные за информационную безопасность назначаются приказом заведующего ДОУ.
- 1.4. Ответственные за информационную безопасность подчиняются заведующему ДОУ.
- 1.5. Ответственные за информационную безопасность в своей работе руководствуются настоящей Политикой.
- 1.6. Ответственные за информационную безопасность в пределах своих функциональных обязанностей обеспечивают безопасность информации, обрабатываемой, передаваемой и хранимой при помощи информационных средств в ДОУ.

**2. Основные задачи и функции ответственных за информационную
безопасность**

- 2.1. Основными задачами ответственных за информационную безопасность являются:
 - 2.1.1. Организация эксплуатации технических и программных средств защиты информации.
 - 2.1.2. Текущий контроль работы средств и систем защиты информации.
 - 2.1.3. Организация и контроль резервного копирования информации.

2.2. Ответственные за информационную безопасность выполняют следующие основные функции:

2.2.1. Разработка инструкций по информационной безопасности: инструкции по безопасной работе в Интернете.

2.2.2. Обучение персонала и пользователей персональным компьютером (далее – ПК) правилам безопасной обработки информации и правилам работы со средствами защиты информации.

2.2.3. Организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в ДОУ.

2.2.4. Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.

2.2.5. Контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём.

2.2.6. Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.

2.2.7. Контроль пользования Интернетом.

3. Обязанности ответственных за информационную безопасность

3.1. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных на них обязанностей. Немедленно докладывать заведующему ДОУ о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принимать необходимые меры по устранению нарушений.

3.2. Совместно с программистами принимать меры по восстановлению работоспособности средств и систем защиты информации.

3.3. Проводить инструктаж работников и пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.

3.4. Формировать и представлять пароли для новых пользователей, администрировать права пользователей.

3.5. Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку компьютеров на наличие вирусов.

3.6. Выполнять регулярно резервное копирование данных на сервере, при необходимости восстанавливать потерянные или поврежденные данные.

3.7. Ежемесячно подавать заведующему ДОУ статистическую информацию по пользованию Интернетом.

3.8. Вести учет пользователей «точки доступа к Интернету». В случае необходимости лимитировать время работы пользователя в Интернете и объем скачиваемой информации.

3.9. Сообщать незамедлительно заведующему ДОУ о выявлении случаев несанкционированного доступа в Интернет.

4.Права ответственных лиц за информационную безопасность

4.1.Требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения.

4.2.Готовить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов.

5.Ответственность лиц за информационную безопасность

5.1.На ответственных лиц за информационную безопасность возлагается персональная ответственность за качество проводимых ими работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определёнными настоящей Политикой.

Локальный акт действует до замены новым.