Принято: на педагогическом совете
Протокол № 4 от «15» 05. 2026 г.

Утверждаю:
Заведующий МБДОУ «Детский сад комбинированного вида № 68» НМР РТ
_____Горшкова Э.М.
Приказ №____от «___»_____2026 г.

Учтено: мотивированное мнение родителей (законных представителей) МБДОУ «Детский сад комбинированного вида № 68» НМР РТ
Протокол заседания родительского комитета № 2
от «23»05.2026 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0099BE8953AB4EAE57A1720F1C285606FD
Владелец: Горшкова Эльмира Мубараковна
Действителен: с 21.05.2026 до 14.08.2027

РУКОВОДСТВОПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ(ИСПДн)

В муниципальном бюджетном дошкольном образовательном учреждении «Детский сад комбинированного вида № 68» Нижнекамского муниципального района Республики Татарстан

Настоящий документ подготовлен в рамках выполнения работ по обеспечению безопасной эксплуатации информационной системы персональных данных (далее - ИСПДн)в муниципальном бюджетном дошкольном образовательном учреждении «Детский сад комбинированного вида № 68» Нижнекамского муниципального района Республики Татарстан (далее - ДОУ).

1. Общие положения

Пользователь ИСПДн (далее - Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных ДОУ.

Пользователем является каждый работник ДОУ, участвующий в рамках своих функциональныхобязанностейвпроцессахавтоматизированнойобработкиинформациии имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

Пользователь несет персональную ответственность за свои действия.

Пользователь в своей работе руководствуется настоящей Инструкцией, Положением о защите персональных данных и другими регламентирующими документами ДОУ.

2. Должностные обязанности

Пользователь обязан:

Знать и выполнять требования настоящей Инструкции и других внутренних распоряжений, регламентирующих порядок действий по защите персональных данных.

Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

Знать и соблюдать установленные требования по режиму обработки персональныхданных,учету,хранениюипересылкеносителейинформации,обеспечению

безопасности ПДн, а также руководящих и организационно- распорядительных документов.

Соблюдать требования парольной политики(раздел3).

Соблюдать правила при работе в сетях общего доступа и(или)международного обмена - Интернет и других (раздел 4).

Обо всех выявленных нарушениях, связанных с информационной безопасностью ДОУ ,а также для получения консультаций по вопросам информационной безопасности необходимо обратиться к администрации ДОУ.

Пользователям запрещается:

-разглашать защищаемую информацию третьим лицам;

-копировать защищаемую информацию на внешние носители без разрешения своего руководителя;

-самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

-несанкционированнооткрыватьобщийдоступкпапкамнасвоейрабочейстанции;

-отключать(блокировать)средства защиты информации;

-обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;

-сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

-привлекатьпостороннихлицдляпроизводстваремонтаилинастройкиАРМбез согласования с ответственным за организацию работы с ПД.

При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <CtrlxAlt><Del> и выбратьопцию <Блокировка>.

Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него функций.

3. Организация парольной защиты

Полная плановая смена паролей в ИСПДн проводится по мере необходимости, но не реже одного раза в год.

Правила формирования пароля:

-пароль не может содержать имя учетной записи пользователя или какую-либоего часть;

-парольдолженсостоятьнеменеечемиз8символов;

-в пароле должны присутствовать символы трех категорий из числа следующих четырех:

а)прописныебуквыанглийскогоалфавитаотАдоZ;б)строчныебуквыанглийского алфавита от a до z;в) десятичные цифры (от 0 до 9);

г)символы,непринадлежащиеалфавитно-цифровомунабору(например,!,$,#,%);

-запрещается использовать в качестве пароля имя входа в систему, простые пароли типа"123","111","qwerty"и им подобные, а также имена и даты рождения своей личности и своих родственников ,клички домашних

животных,номераавтомобилей,телефоновидругиепароли,которыеможноугадать, основываясь на информации о пользователе;

-запрещаетсяиспользоватьвкачествепароляодинитотжеповторяющийсясимвол

Либо повторяющуюся комбинацию из нескольких символов;

-запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

-запрещается выбирать пароли, которые уже использовались ранее.

Правила ввода пароля:

-вводпаролядолженосуществлятьсясучетомрегистра,вкоторомпарольбылзадан;

-во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамерами и др.).

Правила хранения пароля:

запрещается записывать пароли на бумаге, в файле, в электронной записной книжке и на других носителях информации, в том числе на предметах;

запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

Лица, использующие паролирование, обязаны:

-четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

-своевременно сообщать ответственным за организацию работы с ПД об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего доступа и(или)международного обмена

Работа в сетях общего доступа и (или)международного обмена(сети"Интернет"и других) (далее - Сеть) на элементах ИСПДн должна проводиться при служебной необходимости.

При работе в Сети запрещается:

Осуществлять работу при отключенных средствах защиты (антивирусах и других); передавать по Сети защищаемую информацию без использования Средств шифрования;

Посещать сайты сомнительной репутации(порносайты сайты, содержащие нелегально распространяемое ПО, и другие).