

Рекомендовано к утверждению педагогическим советом протокол № 3 от 09.01.2026 г.



ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 140FBAVAA738FFE4715B9739E488FE29  
Владелец: Галеева Лилия Гаязетдиновна  
Действителен с 05.05.2025 до 29.07.2026

Утверждаю директор МБОУ «Ново-Иглайкинская СОШ» Л.Г.Галеева приказ от 09.01.2026 г. № 5

## «Порядок доступа педагогических работников к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, музейным фондам, материально-техническим средствам обеспечения образовательной деятельности»

### 1. Общие положения

1.1. Настоящий Порядок (далее – Порядок) регулирует порядок предоставления, изменения и отзыва прав доступа педагогических работников (далее – ПР) к:

№	Объект доступа	Примеры
1	Информационно-телекоммуникационные сети (корпоративный Wi-Fi, локальная сеть, VPN)	Подключение к школьному серверу, доступ к Интернету через корпоративный шлюз.
2	Базы данных	Электронный журнал, система «УМК», электронные библиотеки, сервисы «Госуслуги в образовании».
3	Учебные и методические материалы	Электронные учебники, методические комплексы, видеоматериалы, презентации, репозитории «Методический центр».
4	Музейные фонды	Цифровые экспозиции, архивные фотографии, 3-D-модели, онлайн-коллекции.
5	Материально-технические (МТ) средства	Компьютерные классы, интерактивные доски, лабораторное оборудование, 3-D-принтеры, проекторы.

### 1.2. Порядок разработан в соответствии с:

№	Нормативный акт	Краткое содержание
1	ФЗ 273-ФЗ «Об образовании в Российской Федерации»	Право родителей и обучающихся на доступ к информации; обязанности школ.
2	ФЗ 294-ФЗ «Об образовании в Российской Федерации (часть 2)»	Права педагогов на использование ИТ-ресурсов.
3	ФЗ 152-ФЗ «О персональных данных»	Защита персональных данных обучающихся и сотрудников.
4	Приказ Минобрнауки России от 30.09.2020 № 1085	Порядок организации ИТ-инфраструктуры в школах.
5	Приказ Минобрнауки России от 02.12.2021 № 1155	Требования к защите информации в образовательных организациях.

№	Нормативный акт	Краткое содержание
6	Региональные нормативные акты (Республика Татарстан) о защите информации в образовании.	Уточняющие положения для регионального уровня.

1.3. Порядок обязателен к исполнению всеми педагогическими работниками, ИТ-службой, руководителями подразделений и отделом кадров образовательной организации.

1.4. Порядок распространяется на всех ПР, работающих в образовательной организации, независимо от формы занятости (полный/неполный день, дистанционная работа).

## 2. Термины и определения

Термин	Определение
<b>Педагогический работник (ПР)</b>	Сотрудник, осуществляющий учебную, методическую, научную, воспитательную или административную деятельность в образовательной организации.
<b>Информационно-телекоммуникационная сеть (ИТ-сеть)</b>	Совокупность аппаратных и программных средств, обеспечивающих передачу, хранение и обработку данных (локальная сеть, Wi-Fi, VPN).
<b>База данных</b>	Система хранения и обработки структурированных данных (электронный журнал, система УМК, электронные библиотеки).
<b>Учебный/методический материал</b>	Любой ресурс, используемый в учебном процессе (электронные учебники, методические рекомендации, видеоматериалы).
<b>Музейный фонд</b>	Цифровой или физический набор экспонатов, доступных для образовательных целей (онлайн-коллекции, архивные материалы).
<b>Материально-технические (МТ) средства</b>	Оборудование и технические ресурсы, используемые в учебном процессе (компьютеры, интерактивные доски, лабораторное оборудование).
<b>Уровень доступа</b>	Набор прав (чтение, запись, изменение, администрирование), предоставляемый ПР в конкретном ИТ-ресурсе.
<b>Согласие на обработку персональных данных</b>	Документ, подтверждающий согласие ПР на обработку его персональных данных в рамках ИТ-систем.

## 3. Права и обязанности педагогических работников

Пункт	Права ПР	Обязанности ПР
3.1	Получать доступ к ИТ-ресурсам, необходимым для выполнения своих должностных обязанностей.	Соблюдать правила ИТ-безопасности, не передавать пароли третьим лицам.
3.2	Пользоваться учебными и методическими материалами в соответствии с лицензиями и авторскими правами.	Уважать авторские права, не копировать материалы без разрешения.

Пункт	Права ПР	Обязанности ПР
3.3	Пользоваться МТ-средствами в установленном порядке, соблюдать правила эксплуатации.	Своевременно сообщать о поломках, не использовать оборудование в личных целях без согласования.
3.4	Получать информацию о своих правах и ограничениях в ИТ-системах.	Проходить обязательные инструктажи по ИТ-безопасности (не реже 1 раза в год).
3.5	Требовать от ИТ-службы своевременного восстановления доступа в случае технических сбоев.	Оповещать ИТ-службу о подозрительных действиях (фишинг, несанкционированный доступ).

#### 4. Порядок предоставления доступа

##### 4.1. Этапы

Шаг	Действие	Ответственный	Срок
4.1.1	ПР заполняет <b>Заявку на предоставление доступа</b> (Приложение 1).	ПР	По необходимости.
4.1.2	Руководитель подразделения проверяет обоснованность и подписывает заявку.	Руководитель	1 рабочий день.
4.1.3	ИТ-служба (администратор сети) создает/корректирует учетную запись, назначает <b>уровень доступа</b> в соответствии с заявкой.	ИТ-служба	2-3 рабочих дня.
4.1.4	ИТ-служба фиксирует действие в <b>Журнале регистрации доступа</b> (Приложение 2).	ИТ-служба	Сразу после создания/изменения доступа.
4.1.5	ПР получает уведомление (электронное/бумажное) о предоставленном доступе и инструкцию по безопасному использованию (Приложение 3).	ИТ-служба	В течение 1 рабочего дня после регистрации.
4.1.6	ПР подписывает <b>Согласие на обработку персональных данных</b> (Приложение 4).	ПР	При получении доступа.

##### 4.2. Уровни доступа (пример)

Уровень	Описание	Примеры ресурсов
<b>А</b> (полный)	Чтение, запись, изменение, администрирование.	ИТ-сеть, серверы, база данных «Электронный журнал».
<b>В</b> (ограниченный)	Чтение + запись (без администрирования).	Учебные материалы, методические репозитории.
<b>С</b> (только чтение)	Просмотр без возможности изменения.	Музейные фонды, публичные архивы.
<b>Д</b> (специальный)	Доступ к отдельным МТ-средствам (например, 3-D-принтер).	Лабораторное оборудование, интерактивные доски.

## 5. Порядок изменения и отзыва доступа

Шаг	Действие	Ответственный	Срок
5.1	При изменении должностных обязанностей ПР инициирует <b>Заявку на изменение доступа</b> (Приложение 5).	ПР/руководитель	По мере необходимости.
5.2	Руководитель проверяет необходимость изменения и подписывает заявку.	Руководитель	1 рабочий день.
5.3	ИТ-служба вносит изменения в учетную запись, фиксирует в <b>Журнале регистрации доступа</b> .	ИТ-служба	1-2 рабочих дня.
5.4	При увольнении, переводе, длительном отсутствии (больничный > 30 дней) – инициируется <b>Заявка на отзыв доступа</b> (Приложение 6).	Руководитель/HR	В течение 1 рабочего дня после получения информации.
5.5	ИТ-служба блокирует учетную запись, удаляет/архивирует права, фиксирует в журнале.	ИТ-служба	1 рабочий день.

## 6. Контроль и аудит доступа

6.1. **Журнал регистрации доступа** (Приложение 2) обязателен к ведению и хранению в течение 3 лет.

6.2. **Периодический аудит** (не реже 1 раза в полугодие) проводится ИТ-службой совместно с отделом внутреннего контроля.

6.3. При обнаружении **нарушений** (неавторизованный доступ, попытки изменения прав без согласования) – фиксируется в **Протоколе инцидента** (Приложение 7) и передаётся в руководителя организации для принятия дисциплинарных мер.

## 7. Защита персональных и конфиденциальных данных

Пункт	Требования
7.1	Все персональные данные обучающихся и сотрудников обрабатываются в соответствии с ФЗ 152-ФЗ.
7.2	Доступ к персональным данным имеет только тот ПР, чей уровень доступа <b>В</b> или <b>А</b> и только в рамках выполнения служебных обязанностей.
7.3	При работе с конфиденциальными данными (медицинские карты, результаты тестов) обязательна <b>двухфакторная аутентификация</b> .
7.4	При передаче данных за пределы ИТ-сети (например, в облако) требуется согласование с руководителем ИТ-службы и подписание <b>Соглашения о конфиденциальности</b> (Приложение 8).
7.5	При утрате/компрометации учётных данных ПР обязан немедленно сообщить ИТ-службе (в течение 1 часа).

## 8. Ответственность

Субъект	Нарушения	Последствия
ПР	Использование доступа в личных целях, передача пароля, нарушение правил ИТ-безопасности	Дисциплинарные меры (выговор, штраф, увольнение) в соответствии с ТК РФ и локальными актами.
Руководитель подразделения	Несвоевременное согласование доступа, предоставление избыточных прав	Внутренняя проверка, возможные дисциплинарные меры.
ИТ-служба	Ошибки в назначении уровней доступа, отсутствие регистрации действий	Внутренняя проверка, корректирующие действия, возможные штрафы.
HR/Отдел кадров	Неправильное оформление заявок на отзыв доступа	Корректировка процедур, обучение персонала.

## 9. Порядок внесения изменений в Порядок

9.1. Предложения по изменению Порядка вносятся в письменной форме руководителем организации или ИТ-службой.

9.2. Рассматриваются педагогическим советом, ИТ-службой и отделом кадров.

9.3. Утверждаются приказом директора организации и фиксируются в реестре локальных нормативных актов.

9.4. Обновлённый Порядок доводится до сведения всех ПР (информационным письмом, размещением в личном кабинете).

## 10. Приложения

№	Наименование	Краткое содержание
<b>Приложение 1</b>	<b>Заявка на предоставление доступа</b>	ФИО, должность, подразделение, требуемый ресурс (с указанием уровня доступа), цель, срок действия, подпись ПР и руководителя.
<b>Приложение 2</b>	<b>Журнал регистрации доступа</b>	Таблица: дата, ФИО ПР, ресурс, уровень доступа, действие (создание/изменение/отзыв), подпись ИТ-службы.
<b>Приложение 3</b>	<b>Инструкция по безопасному использованию ИТ-ресурсов</b>	Правила создания паролей, двухфакторная аутентификация, работа с конфиденциальными данными, правила выхода из системы.
<b>Приложение 4</b>	<b>Согласие на обработку персональных данных</b>	Формуляр, где ПР подтверждает согласие на обработку своих персональных данных в ИТ-системах.
<b>Приложение 5</b>	<b>Заявка на изменение доступа</b>	Аналогична Приложению 1, но с указанием текущих прав и требуемых изменений.

№	Наименование	Краткое содержание
<b>Приложение 6</b>	<b>Заявка на отзыв доступа</b>	ФИО, должность, причина (увольнение, перевод, длительный отпуск), список ресурсов, подпись руководителя и HR.
<b>Приложение 7</b>	<b>Протокол инцидента ИТ-безопасности</b>	Описание нарушения, дата/время, задействованные ресурсы, меры реагирования, подписи ответственных.
<b>Приложение 8</b>	<b>Соглашение о конфиденциальности при работе с внешними сервисами</b>	Условия передачи данных в облако, обязательства сторон, сроки хранения, ответственность.
<b>Приложение 9</b>	<b>Шаблон письма-уведомления о предоставлении/отзыве доступа</b>	Текстовое сообщение, которое ИТ-служба рассылает ПР (по электронной почте/личному кабинету).
<b>Приложение 10</b>	<b>Краткая справка о уровнях доступа</b>	Таблица с описанием прав для уровней А, В, С, D (для ознакомления ПР).

### Примеры заполнения ключевых приложений

#### Приложение 1 – Заявка на предоставление доступа

Заявка № _____
Дата: _____
ФИО ПР: _____
Должность: _____
Подразделение: _____
Требуемый ресурс (указать конкретно):
<input type="checkbox"/> ИТ-сеть (Wi-Fi, VPN)
<input type="checkbox"/> База данных «Электронный журнал»
<input type="checkbox"/> Электронные учебники (УМК)
<input type="checkbox"/> Музейный фонд «История Татарстана»
<input type="checkbox"/> МТ-средство «3-D-принтер»
Уровень доступа (отметьте):
<input type="checkbox"/> А – полный
<input type="checkbox"/> В – ограниченный (чтение/запись)
<input type="checkbox"/> С – только чтение
Цель доступа (кратко): _____
Срок действия (дата начала – дата окончания): _____
Подпись ПР: _____ Дата: _____
Подпись руководителя: _____ Дата: _____

Приложение 2 – Журнал регистрации доступа

Дата	ФИО ПР	Должност ь	Ресурс	Урове нь досу па	Действие (создание/изменение/о тзыв)	Подпись ИТ-службы
04.02.20 26	Ивано в И.И.	учитель математи ки	Электронн ый журнал	В	Создание	_____ ____
04.02.20 26	Петро ва А.С.	учитель истории	Музейный фонд «История Татарстан а»	С	Создание	_____ ____

Приложение 3 – Инструкция по безопасному использованию ИТ-ресурсов (выдержка)

1. **Пароль** – минимум 12 символ