ПРИНЯТО	СОГЛАСОВАНО	УТВЕРЖДЕНО
педагогическим советом	Управляющим	приказом директора
протокол №1	советом	МКОУ СОШ № 5
от 28.08.2025	протокол №1	г. Майского
	от 27.08.2025	№302/1 -ОД
		от 29.08.2025

ПОЛОЖЕНИЕ
о регламентации доступа к сети Интернет в муниципальном казенном общеобразовательном учреждении «Средняя общеобразовательная школа №5 г. Майского»

1. Общие положения

1.1. Настоящее Положение определяет порядок предоставления, ограничения и контроля доступа к сети Интернет для сотрудников, учащихся и иных пользователей в МКОУ СОШ №5 г. Майского (далее — Учреждение).

1.2. Цели: обеспечение безопасного, законного и целевого использования Интернета в учебном и административном процессе; защита обучающихся и информационных ресурсов учреждения; профилактика инцидентов информационной безопасности.

1.3. Действие документа распространяется на всех, кто пользуется сетью Учреждения с его оборудования или по удалённому доступу.

2. Термины и определения

- Интернет-доступ — доступ к глобальным ресурсам через сеть Учреждения.
- Пользователь — сотрудник, ученик, родитель, подрядчик, имеющий доступ к сети Учреждения.
- Администратор сети (системный администратор) — уполномоченное лицо, ответственное за настройку, сопровождение и контроль сети.
- Привилегированный аккаунт — учётная запись с расширенными правами (администрирование, конфигурация).

3. Принципы доступа

- Принцип наименьших привилегий: права выдаются только в объёме, необходимом для выполнения служебных/учебных задач.
- Законность и целевое использование: доступ используется в пределах служебных и образовательных обязанностей.

4. Уровни доступа и их описание

4.1. Общедоступный (учебный) — доступ к образовательным ресурсам, электронным библиотекам, порталам для учёбы; предоставляется учащимся и педагогам по умолчанию.

4.2. Ограниченный (административный) — для сотрудников администрации и преподавателей; блокируются развлекательные и рискованные категории сайтов при необходимости.

4.3. Привилегированный — для системного администратора; доступ к конфигурациям сети и оборудования; сопровождается повышенными требованиями к защите (сложные пароли, двухфакторная аутентификация при возможности).

5. Порядок предоставления доступа

5.1. Инициатором выдачи доступа является ответственное лицо (учитель или системный администратор.

5.2. Системный администратор реализует настройку доступа, регистрирует учётную запись и уведомляет инициатора.

6. Ограничения и блокировка контента

6.1. Запрещается доступ к ресурсам с противоправным, экстремистским, порнографическим, азартным и иным вредоносным содержимым.

6.2. Блокируются социальные сети, мессенджеры, игровые ресурсы или отдельные домены в учебное время для учащихся.

7. Технические меры обеспечения безопасности

7.1. Использование прокси-серверов, антивирусного

7.2. Сегментация сети: отдельные VLAN для учебных устройств, административных компьютеров, гостевой сети.

7.3. Обязательное применение уникальных учётных записей и паролей соответствующей стойкости для сотрудников; смена пароля не реже одного раза в 6 месяцев для привилегированных аккаунтов.

7.4. Запрет на подключение к сети несертифицированных сетевых устройств без согласования с системным администратором.

8. Удалённый доступ

8.1. Удалённый доступ (удалённый рабочий стол) предоставляется только сотрудникам по согласованию с директором и системным администратором.

8.2. При использовании удалённого доступа обязательны: защищённые каналы связи, использование учётных данных Учреждения, обновлённое антивирусное ПО на клиентском устройстве.

9. Правила использования Интернета для учащихся и сотрудников

9.1. Интернет используется преимущественно в учебных и служебных целях. Личное использование допускается в свободное от учебного процесса время и в разумных пределах.

9.2. Запрещается:

- использовать Интернет для противоправной деятельности;

- устанавливать и запускать программное обеспечение без разрешения ИТ-администратора;

- использовать несанкционированные VPN/прокси для обхода фильтров;

- распространять персональные данные и конфиденциальную информацию без разрешения;

- посещать запрещённые ресурсы.

9.3. Родители (законные представители) информируются о правилах и несут ответственность за действия несовершеннолетних при пользовании личными устройствами.

10. Реагирование на инциденты

10.1. Любые подозрительные события или нарушения немедленно сообщаются системному администратору и директору.

10.2. При подтверждённом инциденте доступ пользователя может быть временно приостановлен; проводится расследование, по результатам которого принимаются меры (восстановление доступа, дисциплинарные, уведомление родителей/правоохранительных органов при необходимости).

11. Ответственность и дисциплинарные меры

11.1. Нарушение Положения влечёт дисциплинарную ответственность в соответствии с внутренними правилами и трудовым законодательством.

11.2. В отдельных случаях возможно привлечение к административной или уголовной ответственности согласно законодательству.