

ПРИНЯТО

решением Педагогического совета
МБОУ «СОШ № 99 г. Челябинска»
Протокол № 4 от 28.08 2026



ПОЛОЖЕНИЕ
об информационной безопасности и цифровой гигиене обучающихся
в МБОУ «СОШ № 99 г. Челябинска»

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с:

- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»,
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,
- Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»,
- СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания», а также иными локальными нормативными актами школы.

1.2. Положение определяет правила доступа обучающихся к видам информации, распространяемой посредством сети интернет, защиты их от информации, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, регулирует условия и порядок использования сети интернет в организации.

1.3. Действие настоящего Положения распространяется на всех участников образовательного процесса: обучающихся, педагогических работников, родителей (законных представителей) и администрацию школы.

2. Цели и задачи

2.1. Цель: Создание безопасной образовательной среды и формирование у обучающихся устойчивых навыков цифровой гигиены и критического мышления в сети Интернет.

2.2. Задачи:

- Защита обучающихся от доступа к информации, причиняющей вред их здоровью, нравственному и психическому развитию (пропаганда насилия, экстремизма, порнографии, суицида и т.д.).
- Обучение правилам защиты персональных данных и формирования безопасного «цифрового следа».
- Профилактика кибербуллинга (травли в сети), интернет-зависимости и компьютерной аддикции.
- Техническое и программное обеспечение фильтрации интернет-контента в школьной локальной сети.
- Повышение цифровой грамотности педагогов и родителей (законных представителей).

3. Организация информационной безопасности в школе

- 3.1. Доступ обучающихся к сети Интернет в школе осуществляется исключительно через систему контентной фильтрации, соответствующую требованиям приказа Роскомнадзора.
- 3.2. За настройку, обновление и бесперебойную работу системы контентной фильтрации несет ответственность системный администратор (ответственный за информационную безопасность).
- 3.3. Все компьютеры, используемые в образовательном процессе, должны быть оснащены антивирусным программным обеспечением.
- 3.4. Запрещается разглашение третьим лицам баз персональных данных обучающихся и сотрудников школы без их письменного согласия, за исключением случаев, предусмотренных законодательством РФ.

4. Цифровая гигиена: основные правила для обучающихся

4.1. Здоровьесбережение:

- Соблюдение норм экранного времени (согласно СанПиН).
- Использование правила «20-20-20»: каждые 20 минут отвлекаться от экрана на 20 секунд и смотреть на объект, находящийся на расстоянии 20 футов (6 метров).
- Соблюдение правильной осанки и дистанции до экрана (не менее 50 см для мониторов, 30 см для смартфонов).

4.2. Безопасность данных и цифровой след:

- Запрещается передавать свои пароли от учебных порталов и социальных сетей третьим лицам.
- Обучающиеся должны осознавать, что любая информация, опубликованная в сети (фото, комментарии, переписки), формирует «цифровой след» и может быть использована против них в будущем.
- Запрещается публикация фотографий и видео, компрометирующих честь и достоинство других лиц (учеников, учителей), а также размещение геолокации своего дома или школы в открытом доступе.

4.3. Критическое мышление и этика

- Запрещается участие в кибербуллинге, создание травящих сообществ, распространение слухов и оскорблений.
- Обязательная проверка информации из непроверенных источников перед ее пересылкой (профилактика распространения фейковых новостей).
- Запрещается переход по подозрительным ссылкам и скачивание файлов от неизвестных отправителей (защита от фишинга и вирусов).

5. Обязанности участников образовательного процесса

5.1. Администрация школы:

- Обеспечивает техническую защиту сети Интернет и работу контентного фильтра.
- Организует регулярные инструктажи для обучающихся по технике безопасности и информационной безопасности.
- Проводит мониторинг школьных чатов и групп на предмет выявления фактов кибербуллинга и пресекать их.
- Организует просветительскую работу с родителями (законными представителями): родительские собрания, лектории, рассылка памяток.

5.2. Педагогические работники:

- Интегрируют элементы цифровой гигиены и информационной безопасности в учебные предметы (информатика, ОБЗР, литература, классные часы).
- Проводят целевые инструктажи перед использованием сети Интернет на уроках.
- Немедленно информируют администрацию школы и родителей при выявлении фактов кибербуллинга, суицидальных настроений или вовлечения обучающихся в деструктивные интернет-сообщества.

– Не используют личные социальные сети для общения с обучающимися в неурочное время, за исключением официальных учебных чатов, регламентированных локальными актами.

5.3. Обучающиеся:

- Соблюдают правила пользования школьным оборудованием и сетью Интернет.
- Уважают цифровое достоинство одноклассников и педагогов, не участвуют в травле.
- Сообщают учителю или родителям о фактах столкновения с запрещенным контентом, киберпреступлениями или фактами давления в сети.

5.4. Родители (законные представители):

- Контролируют время, проводимое ребенком за экранами устройств, и соблюдают цифровую гигиену дома.
- Обсуждают с ребенком правила безопасного поведения в сети, проявляют интерес к его цифровой жизни.
- Используют средства родительского контроля на домашних устройствах ребенка (при необходимости).
- Немедленно сообщают классному руководителю или администрации школы о фактах травли ребенка в сети или о совершении ребенком противоправных действий в интернете.

6. Ответственность

6.1. Лица, виновные в нарушении правил информационной безопасности, несут ответственность в соответствии с действующим законодательством Российской Федерации и локальными актами школы.

6.2. За разглашение персональных данных, оскорбление личности в сети (кибербуллинг), распространение экстремистских материалов обучающиеся несут дисциплинарную ответственность (вплоть до отчисления из школы в случаях, предусмотренных ФЗ «Об образовании»), а их родители — административную (ст. 5.35 КоАП РФ — Неисполнение родителями или иными законными представителями несовершеннолетних обязанностей по содержанию и воспитанию несовершеннолетних).

6.3. За совершение противоправных действий в сети Интернет (взлом аккаунтов, мошенничество, распространение запрещенной информации) наступает уголовная или административная ответственность в соответствии с законодательством РФ.

7. Заключительные положения

7.1. Настоящее Положение вступает в силу с момента его утверждения директором школы.

7.2. Изменения и дополнения в настоящее Положение вносятся приказом директора школы на основании изменений в законодательстве РФ или по решению Педагогического совета.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 269A368EC9CABEA13C648860D332EECA
Владелец: Чеханина Елена Николаевна, МУНИЦИПАЛЬНОЕ
БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "СРЕДНЯЯ
ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 99 Г. ЧЕЛЯБИНСКА", Директор
Действителен: с 16.09.2025 по 10.12.2026