Муниципальное автономное общеобразовательное учреждение
«Средняя общеобразовательная школа № 10»

ПРИКАЗ

19.08.2024г. № 01-14-410

Об информационной безопасности
МАОУ СОШ № 10

Во исполнения Федеральных законов от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», от 25.07.2002 № 114 –ФЗ «О противодействии экстремистской деятельности», от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в РФ», от 27.07.2006 № 149-ФЗ «Об информатизации, информационных технологиях и о защите информации», Указа президента РФ от 1 июня 2012 г. № 761 «О национальной стратегии действий в интересах детей на 2012 - 2017 годы» и в целях реализации задачи исключения доступа обучающихся к ресурсам сети Интернет, содержащим информацию, причиняющую вред здоровью и развитию детей, не совместимую с задачами обучения и воспитания, а также информацию, распространение которой запрещено на территории Российской Федерации,

ПРИКАЗЫВАЮ:

1. Назначить ответственным за контроль осуществления контентной фильтрации доступа обучающихся к Интернет-ресурсам, причиняющим вред здоровью и развитию детей, а также не совместимых с задачами образования и воспитания заместителей директора по ВР Попову Т.М., Житнткову М.В..

2. Назначить ответственными за контроль использования интернет-ресурсов обучающимися во время свободного доступа к сети Интернет вне учебных занятий:

- в кабинете информатики - учителя информатики;
- в учебных кабинетах, имеющих точку доступа к сети Интернет - учителей-предметников;
- в библиотеке - педагога-библиотекаря.

3. Обеспечить защиту компьютеров от несанкционированного входа и доступа к информации. Разработать систему защитных мер в локальных сетях для предотвращения несанкционированного уничтожения, искажения, копирования, блокирования информации. Ответственный: инженер МАОУ СОШ № 10.

4. Ответственному за контроль осуществления контентной фильтрации доступа обучающихся к Интернет-ресурсам, причиняющим вред здоровью и

развитию детей: проводить обновление контентной фильтрации согласно данным Федерального списка экстремистских материалов, срок исполнения — постоянно. Ответсвенные: заместители директора по ВР Попова Т.М., Житникова М.В..

5. Следить за обновлением Федерального списка экстремистских материалов, ежемесячно производить обновление его печатной версии и проводить проверку поступающей в библиотеку школы литературы, периодических изданий и материалов согласно данному списку, срок исполнения — постоянно. Ответственные: педагоги-библиотекари Загородских О.И., Волохина О.П..

6. Провести инвентаризацию библиотечного фонда и проверить, на всей ли продукции, которую изготовили с 1 сентября 2012 года стоит знак возрастного ограничения. Срок исполнения до 01.09.2024 года. Ответственные: педагоги- библиотекари Загородских О.И., Волохина О.П..

7. Утвердить Правила организации доступа к сети Интернет в МАОУ СОШ № 10. (Приложение №1 к данному приказу).

8. Утвердить Рекомендации по информационной безопасности в МАОУ СОШ № 10. (Приложение №2 к данному приказу).

9. Заместителям директора по ВР довести данный приказ до сведения работников МАОУ СОШ № 10.

10. Контроль за исполнением приказа оставляю за собой.

Директор муниципального
автономного общеобразовательного
учреждения «Средняя
общеобразовательная школа № 10» Ю.М.Неволина

С приказом ознакомлены:
Волохина О.П.
Загородских О.И.
Попова Т.М.
Житникова М.В.

ПРИЛОЖЕНИЕ 1
к приказу от 19.08.2024г. № 01-14-410

ПРАВИЛА ОРГАНИЗАЦИИ ДОСТУПА К СЕТИ ИНТЕРНЕТ В ОО

1. Общие положения

Настоящие Правила регулируют условия и порядок использования сети Интернет через ресурсы общеобразовательного укчреждения (ОУ) обучающимися, учителями и работниками учреждения.

1.1. Использование сети Интернет в ОУ направлено на решение задач учебно-воспитательного процесса.

1.2. Настоящие Правила регулируют условия и порядок использования сети Интернет через ресурсы ОУ обучающимися, педагогическим и работниками и работниками ОУ.

1.3. Использование сети Интернет в ОУ подчинено следующим принципам:

- соответствия образовательным целям;
- содействия гармоничному формированию и развитию личности;
- уважения закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернета;
- приобретения новых навыков и знаний;
- расширения применяемого спектра учебных и наглядных пособий;
- социализации личности, введения в информационное общество.

1.4. Использование сети Интернет в учреждении возможно исключительно при условии ознакомления и согласия лица, пользующегося сетью Интернет в учреждении, с настоящими Правилами.

2. Организация использования сети Интернет в ОУ

2.1. Вопросы использования возможностей сети Интернет в учебно-образовательном процессе рассматриваются на педагогическом совете ОУ.

2.2. При разработке правил использования сети Интернет педагогический совет руководствуется:

- законодательством Российской Федерации;
- опытом целесообразной и эффективной организации учебного процесса с использованием информационных технологий и возможностей Интернета;
- интересами обучающихся;
- целями образовательного процесса.

2.3. Директор ОУ отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в ОУ, а также за выполнение установленных правил. Для обеспечения доступа участников образовательного процесса к сети Интернет в соответствии с установленным в ОУ правилами директор ОУ назначает своим приказом ответственного за контроль осуществления контентной фильтрации доступа обучающихся к Интернет-ресурсам, причиняющим вред здоровью и развитию детей, а также не совместимых с задачами образования и воспитания.

2.4. Во время уроков и других занятий в рамках учебного плана контроль использования обучающимися сети Интернет осуществляет учитель, ведущий занятие. При этом учитель:
- наблюдает за использованием компьютера и сети Интернет обучающимися;
- запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения обучающимся настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в образовательном учреждении;
- принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.
2.6. Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляют: учитель информатики. Учитель информатики:
- наблюдает за использованием компьютера и сети Интернет обучающимися;
- принимает меры по пресечению обращений к ресурсам, не имеющих отношения к образовательному процессу;
- сообщает классному руководителю о преднамеренных попытках обучающегося осуществить обращение к ресурсам, не имеющим отношения к образовательному процессу.
2.7. При использовании сети Интернет в ОУ обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношения к образовательному процессу.
2.8. Пользователи сети Интернет в ОУ должны учитывать, что технические средства и программное обеспечение не могут обеспечить полную фильтрацию ресурсов сети Интернет вследствие частого обновления ресурсов. В связи с этим существует вероятность обнаружения обучающимися ресурсов, не имеющих отношения к образовательному процессу и содержание которых противоречит законодательству Российской Федерации.
2.9. Принципы размещения информации на интернет-ресурсах ОУ призваны обеспечивать:
- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защиту персональных данных обучающихся, педагогических работников и сотрудников ОУ;
- достоверность и корректность информации.
2.10. Персональные данные обучающихся (включая фамилию и имя, класс/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр., иные сведения личного характера) могут размещаться на интернет-ресурсах, создаваемых ОУ, только с письменного согласия родителей (законных представителей обучающихся). Персональные данные педагогических работников и сотрудников ОУ размещаются на его интернет-ресурсах только с письменного согласия лица, чьи персональные данные размещаются.

3. Использование сети Интернет в ОО

3.1. Использование сети Интернет в ОУ осуществляется, как правило, в целях образовательного процесса.
3.2. Обучающемуся запрещается:
- обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);
- осуществлять любые сделки через Интернет;
- осуществлять загрузки файлов на компьютер ОУ без специального разрешения;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.
3.4. При случайном обнаружении ресурса, содержание которого не имеет отношения к образовательному процессу, обучающийся обязан незамедлительно сообщить об этом учителю, проводящему занятие. Учитель обязан зафиксировать доменный адрес ресурса и время его обнаружения и сообщить об этом лицу, ответственному за контроль осуществления контентной фильтрации доступа обучающихся к Интернет-ресурсам, причиняющим вред здоровью и развитию детей, а также не совместимых с задачами образования и воспитания.

4. Права, обязанности и ответственность пользователей:

- Использование сети Интернет в ОУ осуществляется в целях образовательного процесса. - Участники образовательного процесса ОУ могут бесплатно пользоваться доступом к глобальным Интернет-ресурсам по разрешению лица, назначенного ответственным за организацию в ОУ работы сети Интернет и ограничению доступа.
- К работе в сети Интернет допускаются лица прошедшие инструктаж и обязавшиеся соблюдать его.

Правила работы.
Пользователям запрещается:

1. Осуществлять действия, запрещенные законодательством РФ.
2. Посещать сайты, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательства Российской Федерации (порнография, эротика, пропаганда насилия, терроризма, политического и религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности).
3. Загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или

телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

4. Загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом.
5. Передавать информацию, представляющую коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство граждан.
6. Устанавливать на компьютерах дополнительное программное обеспечение, как полученное в Интернете, так и любое другое без специального разрешения.
7. Изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и всех программ, установленных на нем (заставки, картинку рабочего стола, стартовой страницы браузера).
8. Включать, выключать и перезагружать компьютер без согласования с ответственным за организацию в ОУ работы сети Интернет и ограничению доступа.
9. Осуществлять действия, направленные на "взлом" любых компьютеров, находящихся как в «точке доступа к Интернету» ОУ, так и за его пределами.
10. Использовать возможности «точки доступа к Интернету» ОУ для пересылки и записи непристойной, клеветнической, оскорбительной, угрожающей и порнографической продукции, материалов и информации.
11. Осуществлять любые сделки через Интернет.

Пользователи несут ответственность:

1. За содержание передаваемой, принимаемой и печатаемой информации.
2. За нанесение любого ущерба оборудованию в «точке доступа к Интернету» (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность)

Пользователи имеют право:

1. Работать в сети Интернет в течение периода времени, определенного расписанием.
2. Сохранять полученную информацию на съемном диске (дискете, CD-ROM, флеш-накопителе).
3. Размещать собственную информацию в сети Интернет на Интернет-ресурсах ОУ.

1. Иметь учетную запись электронной почты на Интернет-ресурсах ОУ.

ПРИЛОЖЕНИЕ 2
к приказу от 19.08.2024г. № 01-14-410

РЕКОМЕНДАЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

I. Общие положения

1.1. Настоящий документ определяет общие требования по информационной безопасности к работникам ОУ при осуществлении трудовой деятельности.

II. Порядок доступа в ОО

2.1. При наличии технической возможности доступ работников на территорию ОУ должен производиться только с использованием системы контроля и управления доступом ОУ.

2.2. Каждый работник ОУ при входе/выходе в ОУ должен использовать пропуск.

2.3. В случае утери пропуска работники ОУ незамедлительно уведомляют любым доступным способом непосредственного руководителя.

2.4. Работнику запрещается передавать свой пропуск третьим лицам и другим работникам ОУ с целью его использования;

2.5. Доступ на территорию ОУ лиц, не являющихся работниками ОУ, должен производиться в сопровождении того работника, которому необходимо присутствие гражданина для решения рабочих вопросов

III. Защита от несанкционированного доступа в помещениях ОУ

3.1. По окончании рабочего дня, а также в случае одновременного отсутствия всех работников в одном помещении в течении рабочего дня, двери в обязательном порядке должны быть закрыты на ключ.

3.2. В помещениях ОУ должна быть исключена возможность нахождения лиц, не являющихся работниками ОУ при отсутствии визуального контроля со стороны работников ОУ.

IV. Работа с документами и носителями информации

4.1. Запрещается выносить рабочие документы на бумажных или иных носителях информации (флеш-карты, внешние накопители и др.) за пределы территории ОУ без служебной необходимости.

4.2. Уничтожение документов на бумажных носителях должно производиться работниками ОУ только с использованием оборудования ОУ.

4.3. Запрещается утилизировать рабочие документы в урны для мусора, корзины для макулатуры, предварительно не подвергнув их процедуре уничтожения.

4.4. В случае утери рабочих документов и иных носителей информации (флеш-карты, внешние накопители и др.) необходимо

незамедлительно сообщить об этом своему непосредственному руководителю.

4.5. Рекомендуется исключить использование работниками ОУ иностранных облачных ресурсов для совместного редактирования, таких как «Google Docs».

V. Работа с автоматизированными рабочими местами ОУ

5.1. Работникам ОУ необходимо располагать экран монитора в помещении во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами (шторы на оконных проемах должны быть завешаны, жалюзи закрыты);

5.2. При отсутствии визуального контроля Работника за автоматизированным рабочим местом (далее - АРМ) работникам ОУ необходимо блокировать доступ. Для блокировки необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка> либо заблокировать доступ иным способом, предусмотренным в операционной системе.

5.3. Работникам ОУ по окончании рабочего дня необходимо выйти из операционной системы (либо заблокировать АРМ).

5.4. Для предоставления доступа к информационным системам, информационным ресурсам, каналам связи, Работникам ОУ необходимо отправлять заявку в Службу поддержки пользователей по адресу электронной почты spp@permkrai.ru или по телефону +7 (342) 258 22 44.

5.5. Работникам ОУ запрещается самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств (за исключением технических специалистов ОУ).

5.6. Работникам ОУ запрещается не санкционированно открывать общий доступ к каталогам на АРМ, а также производить удаленное подключение к АРМ по незащищенным каналам связи.

5.7. Работникам ОУ запрещается подключать к АРМ личные съемные машинные носители информации и мобильные устройства, а также копировать информацию, ставшую им известной в ходе выполнения должностных обязанностей на такие носители без служебной необходимости.

5.8. Работникам ОУ запрещается отключать (удалять) установленные на АРМ средства защиты информации.

5.9. Работникам ОУ запрещается привлекать лиц, не являющихся работниками ОУ, для осуществления установки программного обеспечения, ремонта или настройки технических средств АРМ (за исключением случаев, когда данные услуги оказываются на договорной основе);

5.10. Работникам ОУ запрещается производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств АРМ (за исключением технических специалистов ОУ).

5.11. Работникам ОУ рекомендуется исключить использование личных автоматизированные рабочие места (ноутбуки, компьютеры) для выполнения своих должностных обязанностей.

5.12. Работникам ОУ запрещается осуществлять фото- и видео съемку рабочих документов, а также публикацию таких документов в социальных сетях и других открытых ресурсах (за исключением случаев, когда это необходимо для выполнения должностных обязанностей).

5.13. Работникам ОУ запрещается производить деструктивные действия в отношении АРМ Учреждения.

5.14. Работникам ОУ необходимо соблюдать правила парольной защиты при работе с АРМ (раздел VI настоящего документа).

5.15. Работникам ОУ необходимо соблюдать правила работы в сети Интернет (раздел VII настоящего документа).

5.16. Работникам ОУ необходимо соблюдать правила антивирусной защиты (раздел VIII настоящего документа).

5.17. Работникам ОУ необходимо не допускать случаев социальной инженерии и фишинга (раздел IX настоящего документа).

VI. Правила парольной защиты

6.1. Требования к паролю

6.1.1 Пароль не должен содержать имя учетной записи пользователя или какую-либо его часть;

6.1.2 Пароль должен состоять не менее чем из 6 символов;

6.1.3 В числе символов пароля обязательно должны присутствовать цифры и буквы как в верхнем, так и нижнем регистрах;

6.1.4 Буквенная часть пароля должна содержать как строчные, так и прописные (заглавные) буквы.

6.1.5. Запрещается использовать в качестве пароля простые пароли, такие как «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о работнике.

6.1.6. Пароль не должен включать в себя легко вычисляемые сочетания символов, а также общепринятые сокращения;

6.1.7. При смене пароля новое значение должно отличаться от предыдущего не менее чем на четыре символа.

6.1.8. Смена пароля должна производиться не реже одного раза в 90 дней, если иное не предусмотрено нормативной документацией ОУ.

6.2. Правила ввода пароля

6.2.1 Ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан.

6.2.2 Во время ввода пароля необходимо исключить возможность его раскрытия иными лицам, в том числе с помощью технических средств (видеокамеры и др.).

6.3. Правила хранения пароля

6.3.1 Рекомендуется не записывать пароль на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

6.3.2 Запрещается сообщать другим работникам и третьим лицам личный пароль от АРМ;

6.3.3 Работникам ОУ необходимо своевременно сообщать непосредственному руководителю об утере, компрометации, несанкционированном изменении паролей.

VII. Правила работы в сети Интернет

7.1. При работе в сети Интернет работник ОО обязан:

7.1.1 Производить работу в сети Интернет исключительно в целях исполнения своих должностных обязанностей;

7.1.2 Противодействовать методам социальной инженерии: не открывать вложения в письмах от неизвестных источников, не переходить по подозрительным баннерам и ссылкам на веб-сайтах, проверять вводимый адрес веб-сайтов на предмет опечаток.

7.1.3 Обращаться к непосредственному руководителю в случае выявления фактов нарушения информационной безопасности.

7.2 При работе в сети интернет работнику ОУ запрещается:

7.2.1 Посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение, торрент-сайты, и т.д.) и скачивать с таких сайтов какие-либо файлы и программное обеспечение.

7.2.2 Нецелевое использование подключения к сети «Интернет» (просмотр фильмов, скачивание игр и т.д.).

7.3 Использование электронной почты

7.3.1 Каждому работнику ОУ при трудоустройстве должен создаваться служебный адрес электронной почты, размещенный на почтовом сервере Единого почтового домена Пермского края, в адресном пространстве permkrai.ru;

7.3.2. При увольнении работника ОУ служебный адрес электронной почты в обязательном порядке подлежит удалению;

7.3.3. Не допускается передача учетных данных (логин, пароль) электронной почты другим работникам ОУ и третьим лицам;

7.3.4. Использовать в служебных целях личные адреса электронной почты запрещается;

7.3.5. Не допускается использование электронной почты для отправки информации содержащей персональные данные;

7.3.6. Не допускается использование электронной почты для отправки конфиденциальной информации, информации ограниченного доступа и информации, содержащей государственную тайну;

7.3.7. Для приема обращений граждан не допустимо использование сторонних почтовых сервисов не отвечающих требованиям безопасности в соответствии с действующим законодательством в области защиты персональных данных;

7.3.8. Для направления ответов на обращения граждан рекомендуется использовать только служебный адрес электронной почты, размещенный на почтовом сервере Единого почтового домена Пермского края, в адресном пространстве permkrai.ru.

7.4. Использование социальных сетей в рабочих целях

7.4 В случае, если должностными обязанностями работника предусмотрено использование социальных сетей («Вконтакте», «Instagram», и др.) (Далее - Приложение) необходимо:

7.4.1 Ознакомиться с политикой использования Приложения;

7.4.2 Не загружать конфиденциальную информаций в Приложение (В т.ч. Персональные данные);

7.4.3 Исключить передачу учетных данных (логин, пароль) третьим лицам и другим работникам ОУ;

7.4.2 В случае наличия технической возможности Приложения использовать двухфакторную аутентификацию.

VIII. Соблюдение антивирусной защиты информации

8.1. Работник ОУ обязан:

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник обязан самостоятельно или совместно с непосредственным руководителем и/или техническим специалистом ОО провести внеочередной антивирусный контроль АРМ;

8.1.2 Производить антивирусную проверку отчуждаемых машинных носителей (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

8.1.3. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов:

- приостановить работу с АРМ;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов непосредственным руководителем и/или техническим специалистом ОУ;

8.1.4 периодически, не реже одного раза в неделю, проводить проверку антивирусом на наличие вирусного заражения (в случаях, если проверка не производится автоматически)

8.2. Работнику ОУ запрещается:

8.2.1 Удалять средства антивирусной защиты, установленные на АРМ;

8.2.2. Вносить изменения в настройки средства антивирусной защиты, установленного на АРМ.

IX. Противодействие социальной инженерии и фишингу

9.1. Социальная инженерия – совокупность приемов и методов, применяемых злоумышленниками, направленных на получение от работника служебной (конфиденциальной) информации;

9.1.1. В целях противодействия социальной инженерии работникам Учреждения необходимо:

- не сообщать по электронной почте и по телефону служебной информации пока не будет установлена личность запрашивающего и его право на доступ к такой информации;
- не осуществлять работу за АРМ и с документами в присутствии посторонних лиц;
- блокировать АРМ (при отсутствии за рабочим местом, при окончании рабочего дня и т.д.);
- в случае попытки посторонних лиц получить от работника служебную (конфиденциальную) информацию, незамедлительно сообщить об этом непосредственному руководителю;

9.2. Фишинг - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам, паролям и т.д.).

9.2.1. В целях противодействия фишингу работникам ОУ необходимо:

- осуществлять проверку адреса любого сайта, который запрашивает идентификационную информацию;
- осуществлять проверку электронной почты отправителя писем;
- не проходить по подозрительным ссылкам и не скачивать подозрительные файлы.
- об утере или компрометации логинов и паролей сообщать ответственному работнику отдела информационной безопасности ОУ.

X. Проведение совещаний в формате Видеоконференции

10.3 Рекомендуется исключить использование работниками ОУ в служебных целях иностранных сервисов для проведения видеоконференций (Zoom, Skype, и др.) в ходе исполнения должностных обязанностей.

XI. Использование облачных ресурсов для хранения информации в служебных целях

11.1 Рекомендуется исключить использование облачных ресурсов для хранения информации, таких как «Google Диск», «Яндекс.Диск» и иных облачных ресурсов.

XII. Удаленная (дистанционная) работа

12.1 При установлении удаленного (дистанционного) режима работы правила настоящей инструкции должны соблюдаться в полном объеме.

XIII. Обработка персональных данных

13.1. Обработка персональных данных работниками ОУ должна производиться с соблюдением требований Федерального закона

от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

XIV. Подготовка технических заданий и проведение закупочных процедур

14.1. Запрещается привлекать к подготовке технических заданий лиц, не являющихся работниками ОУ.

14.2. Запрещается разглашать сведения об осуществлении закупок товаров, работ, услуг для обеспечения государственных нужд в соответствии с Федеральным законом от 05.04.2013 г. N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» до момента их официального опубликования, а именно, извещения, технические задания и иную информацию, относящуюся к процедурам определения поставщика (конкурсную, аукционную документацию и т.д.).

XV. Соблюдение конфиденциальности

15.1. Разглашение работниками ОУ конфиденциальной информации, закрепленной в локальных нормативно-правовых актах ОУ, третьим лицам не допускается.

XVI. Ответственность работника за нарушение правил информационной безопасности

16.1. Ответственность за нарушение правил информационной безопасности несет каждый работник ОУ в пределах своих служебных обязанностей и полномочий.

16.2. На основании ст. 192 Трудового кодекса Российской Федерации работники, нарушающие правила настоящего документа, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

16.3. На основании ст. 238 Трудового кодекса РФ все работники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный ОУ в результате нарушения ими правил настоящего документа.

16.4 На основании ст. 81 Трудового кодекса Российской Федерации с работником может быть расторгнут трудовой договор, в случае разглашения Работником охраняемой законом тайны (коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника.