

- рационально пользоваться ограниченными разделяемыми ресурсами (дисковой памятью компьютеров общего пользования, пропускной способностью локальной сети) и расходными материалами;
- выполнять требования техника, а также лиц, назначенных ответственными за эксплуатацию конкретного оборудования, в части касающейся безопасности работы комплекса сети и оборудования;
- выполнять обязательные рекомендации ответственных лиц по компьютерной безопасности;
- предоставлять доступ к ПК техникам и ответственным лицам для проверки исправности и соответствия установленным правилам работы;
- содействовать техникам и ответственным специалистам в выполнении ими своих служебных обязанностей;
- незамедлительно сообщать технику и ответственному специалисту о замеченных случаях нарушения компьютерной безопасности (несанкционированный доступ к оборудованию и информации, несанкционированное искажение или уничтожение информации);
- отключать ноутбук ежедневно по окончании работы;
- уходя из кабинета блокировать учетную запись ПК;
- выключать мультимедийное оборудование (проектор, интерактивная доска) на переменах;
- хранить доступы к автоматизированным информационным системам в недоступном месте;
- регистрировать заявки на техническое обслуживание и использование информационных ресурсов школы на сайте <http://i.school1273.org/>, за исключением отсутствия доступа к интернету или невозможности включить компьютер;
- ежедневно в рабочие дни просматривать личную электронную почту;
- при получении писем из школьной системы рассылок необходимо обязательно подтверждать прочтение письма, нажатием на ссылку в начале письма;
- при изменении адреса эл. почты необходимо своевременно сообщать руководителю СП информатизации.

2.2. Пользователям запрещается:

- использовать оборудование для деятельности, не обусловленной непосредственными функциональными обязанностями и должностной инструкцией;
- создавать помехи работе других пользователей, помехи работе компьютеров и сети;
- включать, выключать, переключать, перемещать, разбирать, изменять настройку оборудования общего пользования, кроме прямого указания ответственного лица и кроме случаев пожарной опасности, дыма из оборудования, или других угроз жизни и здоровью людей или угроз сохранности имущества;
- подключать к локальной сети новые компьютеры и оборудование без участия техника и ответственного специалиста;
- передавать другим лицам свои личные атрибуты доступа (регистрационное имя и пароль);
- хранить свои личные атрибуты доступа (регистрационное имя и пароль) к любому ресурсу сети в легкодоступном месте (рабочий стол, стенд и т.д.)
- осуществлять доступ к оборудованию и сети с использованием чужих личных атрибутов доступа или с использованием чужого сеанса работы;
- удалять файлы других пользователей на серверах общего пользования;
- осуществлять попытку несанкционированного доступа к компьютерному оборудованию и информации хранящейся на компьютерах и передаваемой по сети;
- использовать, распространять и хранить программы, предназначенные для осуществления несанкционированного доступа, взлома паролей, для нарушения функционирования компьютерного оборудования и компьютерных сетей, а также компьютерные вирусы и любые программы ими инфицированные;
- использовать, распространять и хранить программы сетевого управления и мониторинга без специального разрешения ответственных лиц;
- предоставлять доступ к компьютерному оборудованию ученикам;

- использовать на своих рабочих станциях съемных накопителей и прочих устройств без предварительной проверки на возможные угрозы (проникновение вирусов, вредоносных программ, вероятность физических неисправностей). В случае, когда пользователь не может самостоятельно удостовериться в отсутствии угроз, он может привлечь для анализа техника;
- изменять конфигурацию АРМ (вскрывать ПК, менять, добавлять, удалять узлы и детали);
- удалять или изменять установленное программное обеспечение (ПО);
- устанавливать на свой компьютер ПО, не предназначенное для выполнения непосредственных функциональных обязанностей;
- выполнять действия и команды, результат и последствия которых пользователю не известен;
- производить замену IP адресов;
- запоминать пароли к любым сайтам в браузере.

2.3. Пользователи имеют право:

- на получение надлежащего и исправного АРМ, для выполнения непосредственных функциональных обязанностей;
- подавать заявку на увеличение квот на компьютерные ресурсы и удовлетворение потребностей в расходных материалах, при превышении средних норм должно представляться обоснование;
- вносить предложения по установке бесплатного и приобретению коммерческого программного обеспечения общего пользования;
- вносить предложения по приобретению компьютерного оборудования;
- вносить предложения по улучшению настроек оборудования и программного обеспечения общего пользования, по улучшению условий труда;
- получать консультацию у техника и ответственного специалиста по работе с компьютерным оборудованием, программным обеспечением общего пользования, по вопросам компьютерной безопасности, по использованию автоматизированных информационных систем;
- получать уведомления об изменениях настоящего Положения и правил работы на конкретном оборудовании.

3. Регистрация пользователей и оборудования.

- 3.1. Регистрация нового оборудования подключаемого к сети школы производится у техника, ответственного лица. Оборудование персонального пользования закрепляется за работником, берущим на себя ответственность за его эксплуатацию. Ответственное лицо обязано сообщать специалисту, ведущему учет, о перемещении оборудования в иное помещение, об изменении комплектации, о сдаче в ремонт, о передаче ответственности за оборудование другому лицу.
- 3.2. Регистрация пользователей производится специалистами, ответственными за предоставление доступа к конкретному оборудованию и автоматизированным информационным системам.

4. Ответственность.

- 4.1. Настоящее Положение утверждается директором школы и доводится до сотрудников через руководителей подразделений. В случае конфликта, пользователи обязаны выполнить текущее требование указанных лиц, а затем обратиться к руководству для разрешения конфликта.
- 4.2. Пользователь несет ответственность за сохранение в секрете своих паролей для входа в сетевую среду компьютерных ресурсов школы и автоматизированных информационных систем. Пользователям запрещается действием или бездействием способствовать разглашению своего пароля.

4.3. Лица, виновные в нарушении требований РФ от 27 июля 2006 № 152-ФЗ «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

5. Термины и определения

- 5.1. Локальные сети (ЛС) — это сети, состоящие из близко расположенных компьютеров, чаще всего находящихся в одной комнате, в одном здании или в близко расположенных зданиях. Локальные компьютерные сети, охватывающие некое предприятие и объединяющие разнородные вычислительные ресурсы в единой среде, называют корпоративными.
- 5.2. Сервер — аппаратно-программный комплекс, исполняющий функции хранения и обработки запросов пользователей, не предназначенный для локального доступа пользователей (выделенный сервер, маршрутизатор и другие специализированные устройства) ввиду высоких требований по обеспечению надежности, степени готовности и мер безопасности информационной системы школы.
- 5.3. Рабочая станция — персональный компьютер (терминал), предназначенный для доступа пользователей к ресурсам Автоматизированной системы школы, приема передачи и обработки информации.
- 5.4. АРМ - рабочее место, обеспеченное (укомплектованное) рабочей станцией и средствами периферии (принтер, сканер) имеющее/не имеющее доступ к ресурсам корпоративной сети передачи данных
- 5.5. Автоматизированная система (АС) — совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации и производства вычислений.
- 5.6. Техник — должностное лицо, в обязанности которого входит обслуживание всего аппаратно-программного комплекса школы, управление доступом к сетевым ресурсам, а также поддержание требуемого уровня отказоустойчивости и безопасности данных, их резервное копирование и восстановление.
- 5.7. Пользователь — работник школы, имеющий доступ к информационной системе школы для выполнения должностных обязанностей.
- 5.8. Учетная запись — информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.).
- 5.9. Пароль — секретная строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системе для получения доступа к данным и программам. Пароль является средством защиты данных от несанкционированного доступа.
- 5.10. Изменение полномочий — процесс создания, удаления, внесения изменений в учетные записи пользователей АС, создание, удаление, изменение наименований почтовых ящиков и адресов электронной почты, создание, удаление, изменение групп безопасности и групп почтовой рассылки, а так же другие изменения, приводящие к расширению (сокращению) объема информации либо ресурсов доступных пользователю АС.
- 5.11. . Инцидент – событие, произошедшее в результате компьютерного сбоя или человеческого фактора, приведшее к частичной или полной неработоспособности АРМ или АС.

6. Приложения.

- 6.1. Инструкция пользователя при обработке персональных данных на объектах вычислительной техники (Приложение №1)
- 6.2. Инструкция по работе с ресурсами сети Интернет (Приложение № 2)
- 6.3. Разрешение на вынос (вывоз) материальных ценностей из ГБОУ Школа 31273

Инструкция пользователя при обработке персональных данных на объектах вычислительной техники

1. Общие положения

1.1. Данная Инструкция определяет основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) школы

1.2. Пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ.

1.3. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ и несет персональную ответственность за соблюдение требований руководящих документов по защите информации).

2. Основные обязанности пользователя:

2.1. выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции;

2.2. при работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами;

2.3. соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;

2.4. после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска ПЭВМ;

2.5. оповещать обслуживающий ПЭВМ персонал, а также непосредственного руководителя обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;

2.6. помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;

2.7. при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

3. Пользователю запрещается:

3.1. записывать и хранить персональные данные на неучтенных установленном порядке машинных носителях информации;

3.2. удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

3.3. самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;

3.4. самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;

3.5. осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;

3.6. сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ; 4.7. отключать (блокировать) средства защиты информации;

3.7. производить какие-либо изменения в подключении и размещении технических средств; 4.9. производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.

3.8. оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

4. Права пользователя ПЭВМ:

4.1. Обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий.

4.2. Обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

5. Пользователи ПЭВМ несут ответственность за:

5.1. надлежащее выполнение требований настоящей инструкции;

5.2. соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;

5.3. сохранность и работоспособное состояние средств вычислительной техники ПЭВМ;

5.4. сохранность персональных данных.

*Приложение № 2
к Положению «О порядке использования
информационных ресурсов ГБОУ школа
№1273»*

**ИНСТРУКЦИЯ
по работе с ресурсами сети Интернет.**

Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Сотрудникам ГБОУ Школа №1273 запрещается использовать ресурсы сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей. Структурное подразделение ИТ ГБОУ Школа №1273 оставляет за собой право ограничивать доступ к этим ресурсам сети Интернет, а так же к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

При работе с ресурсами сети Интернет недопустимо:

- разглашение служебной информации ГБОУ Школа №1273, ставшей известной сотруднику школы по служебной необходимости либо иным путем;
- распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;
- публикация, 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.

При работе с ресурсами Интернет запрещается:

- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
- использовать анонимные прокси-серверы.

Сотрудники могут нести дисциплинарную ответственность за нарушение данной инструкции.

