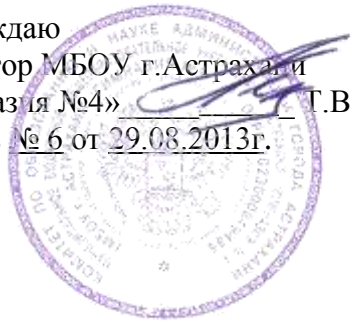
Принято
Педагогическим советом
Протокол №1 от 29.08.2013г.

Утверждаю
Директор МБОУ г.Астрахани
«Гимназия №4» _____ Т.В. Лендова
Приказ № 6 от 29.08.2013г.



ПОЛОЖЕНИЕ
о доступе педагогических работников к информационно-телекоммуникационным сетям, базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения педагогической деятельности, необходимым для качественного осуществления образовательной деятельности гимназии

1. Общие положения

1.1 Настоящее Положение определяет порядок доступа работников гимназии к информационно-телекоммуникационным сетям, базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения педагогической деятельности, необходимым для качественного осуществления образовательной деятельности гимназии.

1.2 Настоящее Положение разработано на основании:

- Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Устава гимназии.

1.3 Доступ педагогических работников к вышеперечисленным услугам осуществляется в целях качественного осуществления ими педагогической, методической и научной деятельности.

1.4 В соответствии с подпунктом 8 пункта 3 ст.47 Федерального закона Российской Федерации от 29 декабря 2012 г. N 273-ФЗ "Об Образовании в Российской Федерации" педагогические работники имеют право на бесплатное получение образовательных, методических и научных услуг оказываемых в МБОУ г. Астрахани «Гимназия №4» (далее - гимназия) в порядке, установленном настоящим положением

1.5 Действие настоящего Положения распространяется на пользователей любого компьютерного оборудования (компьютеры, компьютерная периферия, коммуникационное оборудование), локальной сети гимназии, информационным ресурсам и базам данных, включая информационные библиотечные фонды (далее - ресурсам), а также на пользователей, осуществляющих удаленный доступ к оборудованию локальной сети, информационным ресурсам и базам данных, из других локальных сетей и Интернет.

1.6 В Положении определены права и обязанности пользователей информационно-вычислительной техники, информационных ресурсов и баз данных вне зависимости от прав доступа.

1.7 Несоблюдение Положения работниками может служить основанием для применения дисциплинарного взыскания.

1.8 Настоящее Положение доводится руководителями структурных подразделений до сведения работников при приеме их на работу.

2.Доступ к сетевым ресурсам

2.1 Серверное и сетевое оборудование локальной вычислительной сети гимназии (далее - сети) работает круглосуточно.

2.2 Гарантированный доступ пользователей к информационным и вычислительным ресурсам - с 8.00 до 18.00 в рабочие дни.

2.3 В нерабочие дни и с 18.00 до 8.00 в рабочие дни, ресурсы доступны без гарантии их непрерывной работ, и не несет ответственность за возможную потерю несохраненных данных.

2.4 При профилактиках сетевого оборудования режим доступа регламентируется приказом по гимназии.

3. Порядок оформления доступа к информационным ресурсам

3.1 На новые подключения к ресурсам оформляется заявка, в которой указывается фамилия, имя, отчество, должность, телефон пользователя, ресурс, к которому требуется подключиться, заявка подписывается директором гимназии.

3.2 Пользователь допускается к работе на персональном компьютере (далее - ПК), подключенном к сети, после прохождения инструктажа в БИЦ. Каждому пользователю выдается уникальный идентификатор (логин) и пароль.

4. Порядок подключения компьютеров к сети

4.1. За каждым ПК, подключенным к сети, назначается ответственный, в должностные обязанности которого входит:

• недопущение замены параметров сетевого подключения компьютера или сетевого оборудования без согласования с БИЦ;

• недопущение переключения компьютера в другую розетку сети (за исключением компьютерных классов, где допускается переключение компьютеров в розетки сети в пределах одного помещения).

4.2. В случае увольнения ответственного за ПК, директор гимназии назначает нового ответственного.

5. Обязанности и права пользователей

5.1.Пользователи обязаны:

5.1.1. Ознакомиться с Положением до начала работы на компьютерном оборудовании.

5.1.2. Пройти регистрацию, инструктаж и получить личные атрибуты доступа (имя, пароль) для работы с информационными системами и оборудованием с установленными полномочиями.

5.1.3. Устанавливать личный пароль доступа в соответствии с требованиями к паролям пользователей и порядком работы с ними.

5.1.4. Использовать компьютерное оборудование исключительно для деятельности, предусмотренной производственной необходимостью и должностными инструкциями.

5.1.5. Устанавливать компьютерное оборудование в удобном для работы месте, на прочной (устойчивой) поверхности, вдали от потенциальных источников загрязнения (открытые форточки, цветочные горшки, аквариумы, чайники, вазы с цветами и прочее), так, чтобы вентиляционные отверстия средств вычислительной техники были открыты для циркуляции воздуха.

5.1.6. Протирать оборудование от пыли не реже одного раза в две недели с соблюдением требований ТБ и инструкции по эксплуатации оборудования.

5.1.7. Сообщать о замеченных неисправностях компьютерного оборудования и недостатках в работе программного обеспечения в БИЦ.

5.1.8. Рационально пользоваться ограниченными разделяемыми ресурсами (дисковой памятью компьютеров общего пользования, пропускной способностью локальной сети) и расходными материалами.

5.1.9. Выполнять требования системного администратора, а также лиц, назначенных ответственными за эксплуатацию конкретного оборудования, в части, касающейся безопасности работы в сети.

5.1.10. Выполнять правила работы в вычислительной сети.

5.1.11. Выполнять обязательные рекомендации ответственных лиц по защите информации.

5.1.12. По запросу системного администратора предоставлять корректную информацию об используемых сетевых программах, о пользователях, имеющих доступ к ПК .

5.1.13. Предоставлять доступ к ПК системным администраторам для проверки исправности и соответствия установленным правилам работы.

5.1.14. Содействовать системным администраторам в выполнении ими своих служебных обязанностей.

5.1.15. Незамедлительно сообщать в БИЦ о замеченных случаях нарушения компьютерной безопасности (несанкционированный доступ к оборудованию и информации, несанкционированное искажение или уничтожение информации).

5.2.Пользователям запрещается:

5.2.1. Устанавливать и настраивать какие-либо серверные сервисы общего пользования без согласования с БИЦ.

5.2.2. Использование на компьютерах, подключенных к сети, беспроводных устройств и/или интерфейсов (Wi-Fi, GSM, и др.) для получения доступа одновременно в сеть гимназии и любые другие сети.

5.2.3. Использование оборудования для деятельности, не обусловленной производственной необходимостью и должностной инструкцией.

5.2.4. Создание помех в работе других пользователей, компьютеров и сети.

5.2.5. Подключение к локальной сети новых компьютеров и оборудования без участия системного администратора БИЦ.

5.2.6. Удаление файлов других пользователей на серверах общего пользования.

5.2.7. Осуществление попыток несанкционированного доступа к компьютерному оборудованию и информации, хранящейся на компьютерах и передаваемой по сети.

5.2.8. Использование, распространение хранение ПО, предназначенного для осуществления несанкционированного доступа, взлома паролей, для нарушения функционирования компьютерного оборудования и компьютерных сетей, а также компьютерных вирусов и любых файлов, ими инфицированных.

5.2.9. Использование, распространение и хранение программ сетевого управления и мониторинга без специального разрешения системного администратора БИЦ.

5.2.10. Нарушение правил работы на удаленных компьютерах и удаленном оборудовании, доступ к которым осуществляется через оборудование или сеть подразделения.

5.2.11. Использование съемных накопителей и прочих устройств без их проверки на возможные угрозы (проникновение вирусов, вредоносные программы, вероятность физических неисправностей).

В случае, когда пользователь не может самостоятельно удостовериться в отсутствии угроз, он может привлечь для анализа системного администратора БИЦ.

5.2.12. Изменение аппаратной конфигурации ПК (вскрывать ПК, менять, добавлять, удалять узлы и детали).

5.2.13. Удаление или замена установленного программного обеспечения (ПО).

5.2.14. Установка на свой компьютер ПО не предназначенного для выполнения производственных задач.

5.2.15. Выполнение действий и команд, результат и последствия которых пользователю не известны.

5.2.16. Производить замену IP адресов и других сетевых параметров.

***Пользователи имеют право при наличии технической возможности и обоснования руководителем подразделения*:**

5.2.17. На получение АРМа, технически исправного и соответствующего непосредственно выполняемым функциональным обязанностям.

5.2.18. На подключения к оборудованию общего пользования.

5.2.19. На получение и модернизацию компьютерного оборудования персонального пользования.

5.2.20. Вносить предложения по приобретению компьютерного оборудования.

5.2.21. Вносить предложения по установке бесплатного и приобретению коммерческого программного обеспечения, включая программное обеспечение общего пользования.

5.2.22. Вносить предложения по улучшению настроек оборудования и программного обеспечения общего пользования, по улучшению условий труда.

5.2.23. Получать консультацию у системного администратора по работе с компьютерным оборудованием и программным обеспечением общего пользования, по вопросам компьютерной безопасности.

5.2.24. Получать уведомления об изменениях настоящего Положения и правил работы на конкретном оборудовании.

6. Регистрация пользователей и оборудования.

6.1. Регистрация нового оборудования, подключаемого к сети, производится у системного администратора БИЦ. Оборудование персонального пользования закрепляется за работником, берущим на себя ответственность за его эксплуатацию. Ответственное лицо обязано сообщать системному администратору БИЦ, ведущему учет, о перемещении оборудования в иное помещение, об изменении комплектации, о сдаче в ремонт, о передаче ответственности за оборудование другому лицу.

6.2. Передачей оборудования считается только передача, оформленная по правилам материального учета.

Обязанности и права системного администратора.

6.3. ***Системный администратор обязан:***

6.3.1. Совершенствовать работу оборудования и программного обеспечения для повышения эффективности выполнения пользователями их служебных обязанностей.

6.3.2. Следить за стабильной работой сервера, установленных на них программ и информационных систем.

6.3.3. Предоставлять пользователям информацию, необходимую для работы на компьютерном оборудовании общего пользования.

6.3.4. Доводить до сведения пользователей информацию об изменении правил или режима работы оборудования общего пользования.

6.3.5. Минимизировать время простоя оборудования из-за неполадок и сервисных работ.

6.3.6. Проводить среди пользователей разъяснительную работу по вопросам компьютерной безопасности.

6.3.7. Доводить до сведения пользователей правила работы на конкретном оборудовании.

6.3.8. Не разглашать информацию, полученную в ходе выполнения служебных обязанностей и не имеющую прямого отношения к выполняемым обязанностям.

6.4. ***Системный администратор имеет право:***

6.4.1. Делать предупреждения пользователям, нарушившим установленные правила работы, а также информировать руководство о произошедшем инциденте.

6.4.2. Требовать от пользователя подробного отчета о работе, если во время этой работы произошел отказ или сбой оборудования или программного обеспечения общего пользования.

6.4.3. Проверять исправность компьютеров, подключенных к сети, правильность настройки сетевых программ и соблюдение правил работы с использованием, при необходимости, административного доступа к ПК на время проверки.

6.4.4. Оперативно отключать от сети, блокировать работу или выводить из эксплуатации оборудование в случае нарушения компьютерной безопасности, по причине неисправности или грубого нарушения правил работы.

6.4.5. Осуществлять экстренное отключение оборудования в отсутствие ответственного лица или пользователя и без предварительного уведомления, для обеспечения бесперебойной работы сети и компьютеров общего пользования.

6.4.6. Удалять без предупреждения файлы пользователей, содержащие игровые программы и программы, предназначенные для нарушения компьютерной безопасности, файлы, зараженные компьютерными вирусами, или содержащие мультимедиа - информацию, не имеющую отношения к образовательной деятельности гимназии.

7. Общие правила работы

7.1. Требования к паролям пользователей и порядок работы с ними:

7.1.1. Пароли должны генерироваться специальными программными средствами либо выбираться самостоятельно пользователями, а при необходимости - администраторами с учетом следующих требований:

- длина пароля пользователя должна составлять не менее 6 символов, если не

предъявляются специфические требования программным обеспечением;

• в составе символов пароля обязательно должны присутствовать буквы и цифры;

• в составе символов пароля желательно использовать знаки пунктуации, специальные символы (" ~ ! @ # $ % &*()- + _ = \! / ?).

7.1.2. Пароль не должен содержать:

• фамилии, имени, отчества пользователя ни в каком виде, т.е. написанными в строчном, прописном, смешанном виде, задом наперед, два раза и т.д.;

• фамилий, имен, отчеств родных и близких пользователя ни в каком виде;

• кличек домашних животных, номеров автомобилей, телефонов и других значимых сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

• известных названий, словарных и жаргонных слов;

• последовательности символов и знаков (111, qwerty, abed и т.д.);

• общепринятых сокращений и аббревиатур (ЭВМ, ЛВС, USER и т.д.);

наименования учетной записи пользователя.

7.2. Ввод пароля

При вводе пароля пользователю необходимо исключить возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерам и т.п.).

7.3. Хранение пароля

7.3.1. Запрещается записывать пароли на бумаге, в файлах, электронных записных книжках и других носителях информации, в том числе на каких либо предметах.

7.3.2. Запрещается сообщать пароли другим пользователям, обслуживающему персоналу информационных автоматизированных систем и регистрировать их в системах под своей учетной записью.

7.3.3. Запрещается пересылать пароль открытым текстом в сообщениях электронной почты.

7.3.4. Хранение своего пароля на бумажном носителе допускается только в личном сейфе владельца пароля.

7.4. Смена паролей

7.4.1. Плановая смена паролей должна проводиться не реже одного раза в год или по требованию политики программного обеспечения.

7.4.2. Для автоматизированных систем (АС), позволяющих настраивать политику парольной защиты и доступа пользователей, используются следующие принципы смены паролей:

• при создании учетной записи администратор устанавливает опцию, регулирующую период смены пароля;

• смена пароля производится пользователем самостоятельно в соответствии с предупреждением системы, возникающим при приближении к сроку окончания действия текущего пароля.

7.4.3. Для АС, в которых отсутствует возможность настройки политики парольной защиты и доступа пользователей, смена паролей осуществляется администратором, путем генерации нового пароля. Передача созданного пароля пользователю осуществляется способом, исключающим его компрометацию.

7.5. Действия в случае утери или компрометации пароля.

7.5.1. В случае утери или компрометации пароля Пользователь обязан незамедлительно поставить в известность администратора сети и предпринять меры по смене пароля: сменить его самостоятельно, либо оформить заявку на смену пароля в адрес системного администратора БИЦ.

Устная заявка Пользователя на смену пароля не является основанием для проведения таких изменений.

8. Ответственность

8.1. Пользователь несет ответственность за сохранение в секрете своих паролей. Пользователям запрещается действием или бездействием способствовать разглашению своего пароля.

8.2. Пользователь несет ответственность за нарушение корректности технологического процесса подсистемы или АРМа и (или) правил доступа к информационным ресурсам, влекущее за собой искажение информации в ресурсах.

8.3. Пользователь несет ответственность за достоверность, актуальность, полноту и соответствие вводимой и отчетной информации в базы данных информационных ресурсов.

8.4. Администрация гимназии несет ответственность за достоверность, полноту и своевременность обновления информации об ОУ на официальном сайте гимназии.

8.5. Администрация гимназии не несет ответственности за противоправные или неэтичные действия в сфере компьютерных или телекоммуникационных технологий, если таковые действия совершены во внеслужебное время и с территории и посредством оборудования, не находящихся под юрисдикцией гимназии. В данной ситуации ссылки такого лица (лиц) на принадлежность к ОУ не могут служить основанием для судебного преследования ОУ.

8.6. Администрация гимназии также не несет ответственности за самостоятельную установку пользователем программного обеспечения, не входящего в утвержденный перечень, а также за ненадлежащую и некачественную работу данного ПО.

8.7. Устранение всех возможных неполадок и сбоев в работе компьютерных ресурсов гимназии, возникших по причине самостоятельной установки работником ПО, не входящего в утвержденный перечень, или в результате нерационального использования техники, осуществляется за счет собственных средств пользователя.

8.8. Администрация гимназии не несет ответственности за самостоятельное размещение пользователем учебных материалов на информационных ресурсах гимназии (школьном сайте и т.д.), за их качество и соблюдение пользователем авторских прав.