Государственное профессиональное образовательное учреждение
Ярославской области
Переславский колледж им. А. Невского

ПРИНЯТО
Советом колледжа
Протокол №
От «15» октября 2018 г.
Председатель Совета колледжа
_____ Е.В. Белова

УТВЕРЖДАЮ
Директор ГПОУ ЯО Переславский
колледж им. А. Невского
_____ Е.В. Белова
приказ № 695 от 16 октября 2018 г.
Регистрационный № _____

ПОЛОЖЕНИЕ
о работе в локальной вычислительной сети в государственного профессионального образовательного учреждения Ярославской области Переславского колледжа им. А. Невского

1. Общие положения

1.1. Настоящее Положение является документом, определяющим основные требования, обязательные для исполнения при работе на персональных компьютерах (ПК) и с мультимедийным оборудованием (ММО) в локальной вычислительной сети (ЛВС) Переславского колледжа им. А. Невского (далее – колледжа).

1.2. Положение распространяется на выполнение всех работ посредством ПК и ММО на территории колледжа.

1.3. Все сотрудники колледжа и обучающиеся в колледже (в дальнейшем - пользователи) допускаются к работе на ПК и ММО только после ознакомления с настоящим Положением и Инструкцией по предоставлению доступа к сети и работе с антивирусными программами под роспись в ведомости (Приложение 1). Ответственность за ознакомление с Положением несет руководитель центра информационных технологий и электронных образовательных ресурсов (ИТ и ЭОР).

1.4. Контроль за исполнением требований настоящего Положения возлагается на руководителя центра ИТ и ЭОР.

2. Требования к организации работы с ПК и ММО

2.1. Требования к ПК и ММО, используемым пользователями на территории колледжа:

- все ПК и ММО должны быть подключены к ЛВС; запрещается подключать личные ПК к ЛВС колледжа;
- на ПК отсутствуют или отключены разъемы USB для работы со сменными носителями информации (флэш-носители, SD-карты, внешние жесткие

диски) за исключением ПК администрации колледжа; запрещается подключать личные носители информации к ПК;
- съемные крышки системных блоков ПК опечатаны печатью руководителя центра ИТ и ЭОР, исключая несанкционированный доступ к оборудованию ПК;
- ПК имеет паспорт с перечнем входящего в него основного оборудования (техническими характеристиками), установленным системным и прикладным программным обеспечением;
- составлен список пользователей ПК, допущенных к работе с указанием ответственного лица за эксплуатацию данного ПК;
- антивирусное ПО установлено на сервере; обновление ПО производится согласно расписания (ежесуточно);
- вход в BIOS ПК закрыт паролем; отключена загрузка ПК с внешних носителей (FDD, CD, LAN);
- смена пароля пользователей на доступ к ПК производится не реже 1 раза в 6 месяцев (один раз в семестр в начале обучения);
- права "администратора" ПК предоставлены только у сотрудникам центра ИТ и ЭОР;
- доступ к папке для обмена файлами по ЛВС предоставлен пользователям только для записи и чтения.

2.2 Решение об изменении предъявляемых требований к отдельным ПК принимается руководителем центра ИТ и ЭОР по мотивированному ходатайству руководителя подразделения.

2.3. Перечень данных ПК, входящих в состав ЛВС колледжа хранится в центре ИТ и ЭОР.

2.4. Копирование информации на ПК, установку ПО, оборудования и драйверов выполняют сотрудники центра ИТ и ЭОР.

3. Порядок предоставления прав доступа к ПК, ресурсам и программам ЛВС

3.1. Предоставление прав доступа сотрудникам колледжа к необходимым для работы программам и сетевым ресурсам ЛВС (в т.ч. к Интернету) выполняется по заявке руководителя структурного подразделения в соответствии с матрицей полномочий (Приложение 2). При изменении должностных обязанностей сотрудника руководитель структурного подразделения направляет в центр ИТ и ЭОР служебную записку на аннулирование прав доступа.

3.2. Предоставление прав доступа обучающимся колледжа к необходимым для работы программам и сетевым ресурсам ЛВС (в т.ч. к Интернету) выполняется по заявке куратора группы (преподавателя, проводящего занятия в данной группе) в начале семестра (Приложение 3). По окончанию учебы в колледже, при отчислении, при переводе на другую специальность, куратор группы (преподаватель, делавший заявку на

подключение) сообщает руководителю центра ИТ и ЭОР – при этом учетная запись и сетевой ресурс обучающегося удаляется.

Каждый студент получив логин-пароль обязан зарегистрироваться:
- в адресной строке браузера набрать: www/adm/local/
- в верхнем меню выбрать раздел «Студенты»
- в открывшемся списке групп выбрать свою группу, например «Группа 2018-BED»
- в списке паролей найти выданный Вам пароль, например «st2328» и кликнуть его мышкой
- нажать кнопку изменить и в открывшемся окне заполнить окна «Фамилия:», «Имя:» и «Специальность:»
- сохранить введенные данные и выйти из программы.

3.3. Предоставление прав доступа к ресурсам ЛВС лицам, не являющимся сотрудниками колледжа может быть предоставлен только по служебной записке в центр ИТиЭОР, с указанием директора колледжа. В служебной записке отражается наименование ресурса ЛВС, причина предоставления доступа, период, на который необходимо предоставить доступ, фамилия, имя, отчество и паспортные данные лица, которому предоставляется доступ..

3.3. Руководитель структурного подразделения своим распоряжением определяет перечень сотрудников отдела, имеющих доступ к каждому конкретному ПК.

3.4. Постоянный доступ к сети Интернет и личным учетным записям, а также сетевым папкам закрепленными за пользователями сети предоставляется по письменному указанию директора колледжа.

4. Пользователям запрещается

4.1. Использовать компоненты программного и аппаратного обеспечения в неслужебных целях.

4.2. Посещать в Интернет сайты, содержащие информацию, не входящую в круг служебных обязанностей работника.

4.3. Получать и отправлять по электронной почте программное обеспечение без согласования с сотрудниками центра ИТ и ЭОР;

4.4. Изменять параметры сетевой идентификации компьютера (имя, IP адрес);

4.5. Предоставлять права удаленного доступа к системным ресурсам своего ПК (корневой раздел жесткого диска, на котором установлена операционная система, каталоги, в которых установлена операционная система);

4.6. Самовольно вносить какие-либо изменения в конфигурацию программно-аппаратных средств ПК или устанавливать дополнительно любые системные программные и аппаратные средства, не предусмотренные паспортом ПК;

4.7. Отключать ПК от ЛВС;

4.8. Нарушать пломбу с компьютера;

4.9. Предоставлять закреплённый за ними ПК в пользование другим лицам или сотрудникам, не имеющим права доступа согласно настоящего положения за исключением сотрудников центра ИТ и ЭОР;

4.10. Записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (флеш-накопители, SD-карты, внешние жесткие диски);

4.11. Оставлять включенный без присмотра ПК, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

4.12. Использовать и хранить на рабочих местах съемные носители информации (флэш-накопители, SD карты, внешние жестки диски и т.п., в том числе цифровые фото и видеокамеры, смартфоны) без специального разрешения;

4.13. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению конфликтной ситуации. Об обнаружении такого рода ошибок ставить в известность ответственного за безопасность информации и руководителю центра ИТ и ЭОР.

4.14. Предпринимать попытки взлома компьютерной защиты ПК других пользователей, ЛВС Техникума, ресурсов сторонних организаций;

4.16. Предпринимать действия, направленные на несанкционированное получение прав доступа к программам, базам данных и иной информации, хранящейся в ЛВС, на ПК других пользователей;

4.17. Сообщать кому бы то ни было, кроме непосредственного руководителя (записывать в доступном месте), свой пароль (пароли);

4.18. Посылать в электронном виде информацию, содержащую сведения ограниченного распространения без применения программного обеспечения для ее защиты;

4.19. Использовать файлы полученные по почте, через Интернет или со сменных носителей без предварительной проверки на наличие вирусов;

4.20. Получать и использовать удалённый доступ на управление ПК других пользователей и серверов.

5. Действия при возникновении неисправностей

5.1. В случае неправильной работы программного обеспечения, обнаружении вирусов, технической неисправности ПК ставить в известность сотрудников центра ИТ и ЭОР.

5.2. В случае проблем при работе с Интернет, электронной почтой обращаться в центр ИТ и ЭОР.

6. Разграничение ответственности по информационной безопасности

6.1. Ответственность за безопасность загруженной информации через Интернет и электронную почту, возлагается на пользователя осуществившего приём этой информации.

6.2. Ответственность за загружаемую информацию пользователем из числа обучающихся во время проведения занятий возлагается на руководителя занятия (мастера практического обучения). Обучающимся запрещается использовать ПК без контроля руководителя занятия.

6.2. Ответственность за информационную безопасность при работе в ЛВС колледжа, установку и обновление сетевого антивирусного программного обеспечения, своевременную установку ПО возлагается на сотрудников центра ИТ и ЭОР.

7. Контроль за соблюдением требований по обеспечению информационной безопасности

7.1. Контроль за соблюдением требований по обеспечению информационной безопасности осуществляют сотрудники центра ИТ и ЭОР.

7.2. Использование пользователями ПК, доступа в Интернет и электронной почты может наблюдаться, протоколироваться и периодически проверяться.

7.3. В целях проведения проверок устойчивости компьютерной защиты, соблюдения пользователями требований настоящего Положения ответственными сотрудниками центра ИТ и ЭОР могут проводиться проверочные мероприятия, не нарушающие целостность и работоспособность аппаратно-программных средств.

8. Ответственность

8.1. За неисполнение требований по информационной безопасности руководители подразделений и пользователи несут административную и дисциплинарную ответственность.

8.2. Ответственность за сохранность пломб, установленных на ПК, несет пользователь ПК. В случае нарушения целостности пломб, руководитель центра ИТ и ЭОР совместно с директором колледжа, проводится служебное расследование, с целью выявления нарушения и составления акта.

Приложение 1

МАТРИЦА ПОЛНОМОЧИЙ
сотрудников структурных подразделений колледжа

№ п/п	Наименование структурного подразделения	Должностное лицо структурного подразделения	Полномочия на право доступа	Фамилия сотрудника

Руководитель центра ИТиЭОР

_____ Шендрик А.Е.

«___» _____ 2018 г.

Приложение 2

ОБРАЗЕЦ ЗАЯВКИ
на выдачу паролей и обеспечение подключения к сети

Руководителю центра ИТиЭОР

Заявка

Прошу Вас выдать логины-пароли и обеспечить подключение к локальной сети колледжа (к сети Интернет) обучающихся группы 20-Б согласно расписанию:

- указать время и период подключения к локальной сети (время, дни недели, месяцы);
- указать время и период подключения к сети Интернет (время, дни недели, месяцы).

Преподаватель кафедры ИС
(роспись) Шендрик А.Е.

03.09.2018 г.

Разработал центра ИТ и ЭОР
_____ Шендрик А.Е

РАССМОТРЕНО
На заседании научно-методического совета
Протокол № 1 от «19 » сентября 2018 г.
Заместитель директора по НМР
_____ А.В. Стоян