Приложение 3
УТВЕРЖДЕНО
Приказ от 23.09.2017г.№ 84-ОД
Директор МКОУ
«СОШ им. С.П. Восканова
с. Пролетарского»
Демченко А.В.

Инструкция
пользователю по защите информации при обработке персональных данных на автоматизированных рабочих местах
в МКОУ «СОШ им. С.П. Восканова с. Пролетарского»

1. Общие положения

1.1. Пользователем является каждый работник, участвующий в рамках своих должностных обязанностей в процессе обработки информации содержащей персональные данные.

1.2. Пользователи допускаются к обработке персональных данных на основании списка утвержденного руководителем и после ознакомления с регламентирующими документами по обеспечению безопасности персональных данных.

1.3. Пользователи несут персональную ответственность за свои действия с персональными данными.

2. Обязанности пользователей

2.1. Пользователи имеют право обрабатывать персональные данные необходимые для исполнения служебной деятельности в соответствии с полномочиями, установленными системным администратором и ответственным за обеспечение безопасности персональных данных.

2.2. Пользователь отвечает за правильностью включения (выключения) автоматизированного рабочего места, вход в систему и все действия при работе на нем.

2.3. Вход в систему осуществляется на основе ввода (по запросу системы) персонального пароля и персональному идентификатору (программному и (или) аппаратному).

2.4. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.5. При временном отсутствии на рабочем месте экран монитора должен быть потушен или использовать экранную заставку, доступ к компьютеру заблокирован.

2.6. Соблюдать правила при работе в сетях общего доступа, антивирусная защита должна всегда быть включена.

3. Пользователям запрещается:

3.1. Разглашать обрабатываемые персональные данные третьим лицам.

3.2. Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

3.3. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

3.4. Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

3.5. Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

3.6. Отключать (блокировать) средства защиты информации.

3.7. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационной системы персональных данных.

3.8. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение безопасности персональных данных.

3.9. Осуществлять ввод персональных данных под диктовку.