654079, Россия, Кемеровская обл.,
г. Новокузнецк, проезд Коммунаров,5
тел.: 97-57-00, 97-57-02
e-mail:licey-11@mail.ru
www.lizey11.ucoz.ru

ИНН4217023667
КПП 421701001
ОКАТО 32431000000
ОГРН 1034217005877

муниципальное бюджетное
нетиповое общеобразовательное учреждение
«Лицей №11»

УТВЕРЖДАЮ:
Директор МБ НОУ «Лицей №11
_____В.Н. Пересыпкин
Приказ №14 «12» января 2015г.

ИНСТРУКЦИЯ
пользователя при обработке персональных данных обучающихся и их родителей (законных представителей) в автоматизированных информационных системах муниципального бюджетного нетипового общеобразовательного учреждения «Лицей №11»

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 автоматизированных рабочих местах (АРМ) Лицея.
1.2. Пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на АРМ.
1.3. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в АРМ и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.
1.4. Сотрудники Лицея и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под расписку с настоящей Инструкцией.

2. Порядок предоставления доступа к работе на АРМ

2.1. Для работы с конфиденциальной информацией каждый пользователь должен получить соответствующий доступ. Под доступом понимается получение каждым пользователем разрешения директора МБ НОУ «Лицей №11» на право работы с защищаемой информацией с учетом его служебных обязанностей (доступ утвержден приказом директора).
2.2. Доступ пользователей к работе на АРМ организует заместитель директора по УВР – А.В. Марков.

3. Основные обязанности пользователя:

3.1. Выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции;
3.2. 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;

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

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

3.4.Оповещать обслуживающий АРМ персонал, а также непосредственного начальника обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в АРМ;

3.5.Не допускать "загрязнение" АРМ посторонними программными средствами;

3.6.Знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий;

3.7.Знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;

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

3.9.Знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов;

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

4. Требования к антивирусной безопасности

4.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции.

4.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

5. Пользователю запрещается:

5.1. Записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;

5.2. Удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

5.3. Самостоятельно подключать к АРМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение АРМ;

5.4. Самостоятельно устанавливать и/или запускать (выполнять) на АРМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;

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

5.6. Сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам АРМ;

5.7. Отключать (блокировать) средства защиты информации;

5.8. Производить какие-либо изменения в подключении и размещении технических средств;
5.9. Производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.
5.10. Оставлять бесконтрольно АРМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

6. Права пользователя АРМ:

6.1. Обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий.
6.2. Обращаться к обслуживающему АРМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в АРМ, а также со средствами защиты информации.

7. Пользователи АРМ несут ответственность за:

7.1. Надлежащее выполнение требований настоящей инструкции;
7.2. Соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;
7.3. Сохранность и работоспособное состояние средств вычислительной техники АРМ;
7.4. Сохранность персональных данных.

Пользователи АРМ, виновные в нарушении законодательства Российской Федерации о защите прав собственности и охраняемых по Закону сведений, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно распорядительными документами.