БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ
ДЛЯ ДЕТЕЙ-СИРОТ И ДЕТЕЙ, ОСТАВШИХСЯ БЕЗ ПОПЕЧЕНИЯ РОДИТЕЛЕЙ,
ВОЛОГОДСКОЙ ОБЛАСТИ «ВЕЛИКОУСТЮГСКИЙ ЦЕНТР ПОМОЩИ ДЕТЯМ,
ОСТАВШИМСЯ БЕЗ ПОПЕЧЕНИЯ РОДИТЕЛЕЙ»

С УЧЕТОМ МНЕНИЯ
Совета учреждения
Протокол от 29.08.2017 №26

УТВЕРЖДАЮ
Директор Н.Н. Долгина
Приказ от 06.09.2017 № 93

ПРАВИЛА ДОСТУПА К ПЕРСОНАЛЬНЫМ КОМПЬЮТЕРАМ, СОДЕРЖАЩИМ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

1. Общие положения

1.1. Правила доступа к персональным компьютерам, содержащим персональные данные (далее – Правила), определяет комплекс организационно-технических мероприятий по обеспечению безопасности персональных данных, хранящихся и обрабатываемых с помощью персональных компьютеров в бюджетном учреждении социального обслуживания для детей-сирот и детей, оставшихся без попечения родителей, Вологодской области «Великоустюгский центр помощи детям, оставшимся без попечения родителей» (далее – Учреждение).

1.2. Правила предназначены для обеспечения эффективной организации защиты персональных данных и содержат требования по обеспечению безопасности персональных данных.

1.3. Пользователь обязан ознакомиться с данными Правилами.

1.4. Ответственность за выполнение требований настоящих Правил, сохранность и правильное использование информации, хранящихся в персональных компьютерах, содержащих персональные данные, несет пользователь и лица, ответственные за обработку персональных данных.

2. Организация работы с персональными компьютерами, содержащими персональные данные

2.1. Лица, допущенные к обработке персональных данных с использованием персональных компьютеров, определяются приказом директора Учреждения.

2.2. Идентификация и авторизация пользователей при работе с персональными компьютерами, содержащими персональные данные, осуществляется в соответствии с Инструкцией об организации парольной защиты персональных компьютеров, содержащих персональные данные.

2.3. С целью обеспечения защиты персональных данных от искажения или уничтожения в случае сбоев в работе вычислительной техники и оборудования ведется резервное копирование защищаемой информации. Периодичность и порядок проведения резервного копирования определяется Инструкцией об организации резервного копирования информации, содержащей персональные данные, обрабатываемой на персональных компьютерах, и контролируется ответственным за резервное копирование, назначенный приказом директора Учреждения.

2.4. При организации своего рабочего места сотрудник так располагает экран

дисплея, чтобы затруднить просмотр информации выведенной на экран посторонним лицам.

2.5. При оставлении по каким-либо причинам своего рабочего места сотрудник обязан заблокировать экран монитора.

3. Возможные угрозы персональным данным, обрабатываемым с использованием персональных компьютеров

3.1. К числу идентифицированных угроз персональным данным, обрабатывающимися с использованием персональных компьютеров, относятся:

- несанкционированный доступ;
- преднамеренные и непреднамеренные сбои в работе средств вычислительной техники, электрооборудования и др., ведущие к потере или искажению информации.

3.2. Несанкционированный доступ к информации – это доступ к информации, нарушающий установленные правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники.

3.3. Несанкционированный доступ к информации может осуществляться:

- зарегистрированными пользователями;
- посторонними лицами, имеющими доступ в помещения, где установлены персональные компьютеры.

3.4. К преднамеренным сбоям относятся сбои в работе оборудования или программного обеспечения, вызванные умышленным воздействием на него с целью уничтожения или искажения информации.

3.5. Непреднамеренные сбои связаны с неисправностью персональных компьютеров, заражением программного обеспечения «вирусами», резкими колебаниями тока в электропитающей сети и т.п., ведущие к уничтожению или блокированию информации.

3.6. Предотвращение возможных угроз персональным данным, обрабатываемым с использованием персональных компьютеров, осуществляется организацией учета, хранения и выдачи информационных носителей, паролей, ключей от кабинетов, где находятся персональные компьютеры.

4. Обязанности пользователей персональных компьютеров, содержащих персональные данные

4.1. Соблюдать соответствующие законодательство Российской Федерации, настоящие Правила, инструкции и другие организационно-распорядительные документы по защите персональных данных.

4.2. Использовать доступные механизмы безопасности для защиты конфиденциальности и целостности их собственной информации.

4.3. Не осуществлять намеренное изменение, уничтожение, чтение, или передачу информации.

4.4. В случае выявления фактов несанкционированного доступа к персональным компьютерам, содержащим персональные данные, блокировки доступа, утери или компрометации пароля и др. пользователь обязан незамедлительно сообщить об этом заместителю директора по административно – хозяйственной работе.

5. Ответственность пользователей персональных компьютеров, содержащих персональные данные

5.1. При нарушениях правил, связанных с безопасностью персональных данных, обрабатываемых с использованием персональных компьютеров, пользователь несет ответственность, установленную действующим законодательством Российской Федерации и нормативными актами Учреждения.

5.2. Пользователь несет ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкционированного использования учетной записи.