Муниципальное автономное
учреждение дополнительного образования
«Центр эстетического воспитания детей «Радуга»

УТВЕРЖДАЮ:
Директор МАУ ДО «ЦЭВД «Радуга»

Н.Н.Паршакова
Приказ № 30 от 28.11. 2015г.

Политика информационной безопасности

Настоящая политика определяет цели и принципы обеспечения информационной безопасности в Муниципальном автономном учреждении дополнительного образования «Центр эстетического воспитания детей «Радуга» (далее МАУ ДО «ЦЭВД «Радуга»). Политика обязательна для исполнения всеми сотрудниками, а также лицами, работающими с информацией, принадлежащей МАУ ДО «ЦЭВД «Радуга» в рамках заключенных договоров.

Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, назначенным приказом директора Учреждения, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

Целями обеспечения информационной безопасности являются минимизация ущерба от реализации угроз информационной безопасности.

Объектом защиты является информация, носитель информации или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации, а также помещения, в которых расположены средства обработки защищаемой информации.

В Учреждении применяются следующие методы защиты информации:

- правовые;
- организационно-технические;
- экономические.

Информационная безопасность охватывает все аспекты работы МАУ ДО «ЦЭВД «Радуга» – от организации внутреннего и внешнего оборота документов до порядка действий в случае возникновения непредвиденных и чрезвычайных ситуаций.

Информация является важным активом Учреждения и ее защита является обязанностью каждого сотрудника.

Основными направлениями обеспечения информационной безопасности следует рассматривать:

- обеспечение информационной безопасности при ведении делопроизводства и осуществлении документооборота (при использовании средств автоматизации, а также без использования средств автоматизации);
- обеспечение информационной безопасности при работе в сети Интернет;
- обеспечение антивирусной защиты;
- обеспечение информационной безопасности при проведении работ по созданию (модернизации) информационных систем;
- обеспечение безопасности конфиденциальной информации;
- обеспечение информационной безопасности при осуществлении взаимодействий с другими организациями;
- обеспечение информационной безопасности при соблюдении правовых и договорных требований;
- обеспечение информационной безопасности в условиях чрезвычайных ситуаций.

▪ Под угрозами информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:
утрата сведений, составляющих защищаемую информацию, а также искажение (несанкционированная модификация, подделка) такой информации;

▪ утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.), а также утечка информации по каналам связи и за счет побочных электромагнитных излучений;

▪ недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств.

Доступ к конфиденциальной информации (в том числе к персональным данным сотрудников, обучающихся, родителей (законных представителей) предоставляется только лицам, которые определены приказом директора МАУ ДО «ЦЭВД «Радуга».

Доступ к информации предоставляется только тем лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.

Для каждого информационного ресурса определяется владелец, отвечающий за предоставление к нему доступа и эффективное функционирование мер защиты информации.

Сотрудники МАУ ДО «ЦЭВД «Радуга» проходят обучение в области информационной безопасности.

Директор МАУ ДО «ЦЭВД «Радуга» утверждает политики информационной безопасности.

В связи с отсутствием в штате Учреждения IT- специалиста, программиста, а также отсутствием Отдела информационной безопасности, обслуживание офисной техники (в том числе компьютеров) ведется сторонними организациями путем заключения договора. Сторонняя организация обязана выполнять все требования российского законодательства в области защиты информации.

Меры защиты информации внедряются по результатам проведения оценки рисков информационной безопасности.

Оценка рисков информационной безопасности проводится ежегодно в начале учебного года (сентябрь-октябрь), а также в случае значительных изменений в структуре Учреждения.

Успешное достижение целей настоящей политики возможно только при выполнении положений следующих детальных политик информационной безопасности:

- Политика использования паролей;
- Политика использования сети Интернет;
- Политика использования электронной почты.

Несоблюдение политик информационной безопасности сотрудниками МАУ ДО «ЦЭВД «Радуга» может повлечь дисциплинарные меры взыскания вплоть до увольнения.