АДМИНИСТРАЦИЯ ОДИНЦОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА МОСКОВСКОЙ ОБЛАСТИ

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬЕНОГО ОБРАЗОВАНИЯ
ОДИНЦОВСКАЯ ДЕТСКАЯ ШКОЛА ИСКУССТВ «КЛАССИКА»

СОГЛАСОВАНО
Протокол заседания
Общего собрания МАУДО
Одинцовской ДШИ
«Классика»
№_1_от 16.01.2019 г.

УТВЕРЖДЕНО
Приказом по МАУДО
Одинцовской ДШИ «Классика».
№_7-ОД_от 16.01.2019 г.
Директор _____ Т.А.Ферафонтова

Положение
об информационной безопасности МАУДО Одинцовской ДШИ «Классика»

1.Общие положения

1.1.Настоящее Положение об информационной безопасности МАУДО Одинцовской ДШИ «Классика» (далее — Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (редакция от 28.06.2010).

1.2.Информационная безопасность Школы включает в себя следующие направления:

- информационная безопасность компьютеров, локальной сети, серверов и информационных систем, которая предполагает защиту от несанкционированного доступа, разграничение прав доступа, защиты от вирусов, и компьютерных атак.
- информационная безопасность персональных данных;

1.3.В настоящем Положении определяются также задачи, функции, обязанности и права лиц, ответственных за информационную безопасность.

2.Информационная безопасность компьютеров, локальной сети, серверов и информационных систем.

2.1. Школа оснащена компьютерной техникой, которая используется:

- **в информационном центре** – библиотекарем и преподавателями школы (2 компьютера);
- **в административных помещениях** –
  директором (1 компьютер),
  ответственным лицом за работу по закупкам и электронным торгам,
  заместителями директора по учебно-воспитательной работе (4 компьютера),
  заместителем директора по АХЧ (1 компьютер),
  заместителем директора по безопасности (1 компьютер),
  заведующим отделением платных образовательных услуг (1 компьютер),
  секретарем учебной части (1 компьютер).
- **в учебных кабинетах заведующих отделами –** (4 компьютера).

2.1.1.Компьютеры директора, заместителей директора по УВР, АХЧ, безопасности, секретаря учебной части, библиотекаря и лица, ответственного за работу по закупкам и электронным торгам, должны быть подключены к сети Интернет.
Компьютеры в учебных кабинетах не подключаются к сети Интернет и предназначены для подготовки учителей к урокам и к работе на уроке с мультимедийным проектором.
2.1.2.Компьютер, на котором работает лицо, ответственное за работу по закупкам и электронным торгам, должно стоять специальное ПО для работы с ЭЦП для АИС ГЗ и АИС «Электронный торги», настроен официальный электронный адрес Школы.
2.1.3. На всех компьютерах должно стоять полноценное антивирусное ПО, защищающее от вирусов, троянов, сетевых атак и т.п.
2.1.4.Администрация Школы должна издать приказы, в которых назначаются ответственные за работу с информационными системами, а также приказ о назначении ответственного за информационную безопасность Школы. В этих приказах указываются конкретные фамилии.

2.2.Основные задачи и функции лиц, ответственных за информационную безопасность.

2.1.Ответственные за информационную безопасность:
- назначаются приказом директора школы;
- руководствуются настоящим Положением;
- обеспечивают безопасность информации, обрабатываемой, передаваемой и хранимой при помощи информационных средств в школе.

2.2.Основными задачами ответственных за информационную безопасность являются:
- организация эксплуатации технических и программных средств защиты информации;
- текущий контроль работы средств и систем защиты информации;
- организация и контроль резервного копирования информации.

2.3.Ответственные за информационную безопасность совместно с организацией, заключившей договор на обслуживание компьютерной техники Школы, выполняют следующие основные функции
- разработка инструкций по безопасной работе в Интернете, информационной безопасности, организации антивирусной защиты,
- обучение пользователей персональным компьютером (далее – ПК) правилам безопасной обработки информации и правилам работы со средствами защиты информации;
- антивирусный контроль магнитных носителей информации и файлов электронной почты, поступающих в Школу;
- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации;
- контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём;
- контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК;
- контроль пользования Интернетом.

2.3.Обязанности лиц, ответственных за информационную безопасность

Лица, назначенные приказом директора ответственными за информационную безопасность, совместно с организацией, заключившей договор на обслуживание компьютерной техники Школы, должны:
- контролировать обеспечение функционирования и поддержки работоспособности средств и систем защиты информации в пределах возложенных на них обязанностей;
- немедленно докладывать директору о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принимать необходимые меры по устранению нарушений;

- проводить с помощью обслуживающей организации инструктаж сотрудников и пользователей ПК по правилам работы с используемыми средствами и системами защиты информации;
- администрировать права пользователей;
- отслеживать работу антивирусных программ, проводить в неделю полную проверку компьютеров на наличие вирусов;
- выполнять периодическое резервное копирование данных на сервере, при необходимости восстанавливать потерянные или поврежденные данные.

2.4.Права ответственных лиц за информационную безопасность

Лица, назначенные приказом директора ответственными за информационную безопасность имеют право:

- требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения и электронных платежей;
- готовить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов.

3.Обеспечение информационной безопасности персональных данных участников образовательного процесса школы

3.1.В школе должен быть разработан и утвержден перечень необходимых документов, регламентирующих работу с персональными данными участников образовательного процесса – сотрудниками, обучающимися, родителями (законными представителями обучающихся):

- ✓ Положение об обработке персональных данных работников Школы (ПДн);
- ✓ Согласие работника школы на обработку своих персональных данных;
- ✓ Положение об обработке персональных данных обучающихся;
- ✓ Согласие законного представителя обучающегося (до 18 лет) в школе на обработку персональных данных обучающегося;
- ✓ Положение о службе информационной безопасности школы;
- ✓ Положение об ответственности работников, допущенных к обработке персональных данных;
- ✓ Обязательство работника о неразглашении персональных данных;
- ✓ Приказ о назначении ответственных лиц за ПДн и список ответственных лиц.
- ✓ Приказ о введении режима обработки ПДн.
- ✓ Перечень подразделений и сотрудников, допущенных к работе с ПДн.
- ✓ Перечень ПДн.
- ✓ Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах.

3.2.Ответственными лицами за безопасность ПДн назначаются, как правило, секретарь учебной части, заместители директора по УВР; из них же создается рабочая группа.

3.3.Рабочая группа действует в рамках вышеперечисленных локальных актов: