РАССМОТРЕНО и ПРИНЯТО
на педагогическом совете школы
протокол № 01
от «28» августа 2018 г.

УТВЕРЖДЕНО
директор
ГБНОУ «РООМХШИ им. Р.Д. Кенденбиля»
_____ А.-Х.Д. Балбан-оол
Приказ № 21 от "01" сентября 2018 г.

ПОЛОЖЕНИЕ
об информационной безопасности

Государственного бюджетного нетипового общеобразовательного учреждения «Республиканская основная общеобразовательная музыкально-художественная школа-интернат им. Р.Д. Кенденбиля»
(Республиканская школа искусств)

1. Общие положения

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности Государственного бюджетного нетипового общеобразовательного учреждения «Республиканская основная общеобразовательная музыкально-художественная школа-интернат им. Р.Д. Кенденбиля» (далее школа). Под информационной безопасностью школы следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

1.2. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

1.3. К объектам информационной безопасности в школе относятся:

1.3.1. Информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;

1.3.2. Информация, защита которой предусмотрена законодательными актами РФ, в т. ч. и персональные данные;

1.3.3. Средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

1.4. Система информационной безопасности должна обеспечивать:

1.4.1. Конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);

1.4.2. Целостность (точность и полноту информации и компьютерных программ);

1.4.3. Доступность (возможность получения пользователями информации в пределах их компетенции).

1.5. Обеспечение информационной безопасности осуществляется по следующим направлениям:
1.5.1. Правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
1.5.2. Организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
1.5.3. Инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

2. Правовые нормы обеспечения информационной безопасности.

2.1. Школа имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных учащихся, работников школы, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.
2.2. Школа обязана обеспечить:
2.2.1. Сохранность конфиденциальной информации.
2.2.2. Запрет на распространение информации, негативно влияющей на несовершеннолетних, запрещенной к распространению в соответствии с Федеральным законом №114-ФЗ от 25 июля 2002 «О противодействии экстремистской деятельности»;
2.2.3. Защиту информационных ресурсов сайта от размещения на них информации несовместимой с целями и задачами образовательного процесса.
2.3. Администрация школы:
2.3.1. Назначает ответственного за обеспечение информационной безопасности;
2.3.2. Издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
2.3.3. Имеет право включать требования по обеспечению информационной безопасности в коллективный договор;
2.3.4. Имеет право включать требования по защите информации в договоры по всем видам деятельности;
2.3.5. Имеет право требовать защиты интересов школы со стороны государственных и судебных инстанций.
2.4. Организационные и функциональные документы по обеспечению информационной безопасности:
2.4.1. Приказ руководителя школы о назначении ответственного за обеспечение информационной безопасности;
2.4.2. Должностные обязанности ответственного за обеспечение информационной безопасности;
2.4.3. Перечень защищаемых информационных ресурсов и баз данных;

2.4.4. Инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников школы и др.
2.5. Порядок допуска сотрудников школы к информации. Такой допуск предусматривает:
2.5.1. Принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
2.5.2. Ознакомление работника с нормами законодательства РФ и школы об информационной безопасности и ответственности за разглашение информации конфиденциального характера.

3. Мероприятия по обеспечению информационной безопасности.

3.1. Для обеспечения информационной безопасности в школе требуется проведение следующих первоочередных мероприятий:
3.1.1. Защита интеллектуальной собственности школы;
3.1.2. Защита компьютеров, локальных сетей и сети подключения к системе Интернета в классе информатики;
3.1.3. Организация защиты конфиденциальной информации, в т. ч. персональных данных работников и учащихся школы;
3.1.4. Учет всех носителей конфиденциальной информации.
3.2. Обладатель информации, ведущий администратор информационной системы обязан обеспечить:
3.2.1. Предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
3.2.2. Своевременное обнаружение фактов несанкционированного доступа к информации;
3.2.3. Предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
3.2.4. Недопущения воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
3.2.5. Возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
3.2.6. Постоянный контроль за обеспечением уровня защищенности информации.

4. Организация работы с информационными ресурсами и технологиями.

4.1. Система организации делопроизводства:
4.1.1. Учет всей документации школы, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
4.1.2. Регистрация и учет всех входящих (исходящих) документов школы в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);

4.1.3. Особый режим уничтожения документов. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

- Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.
- Документы, дела и издания с грифом «Для служебного пользования» должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.
- Выданные для работы дела и документы с грифом «Для служебного пользования» подлежат возврату в тот же день.
- Передача документов исполнителю производится только через ответственного за документацию.
- Запрещается выносить документы с грифом «Для служебного пользования» за пределы школы.
- При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

5. Нормативные документы.

Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.).
Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
Федеральный закон №114-ФЗ от 25 июля 2002 «О противодействии экстремистской деятельности».
Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ.