СОГЛАСОВАНО: «Утверждаю»

на педагогическом совете Директор Мраморной СОШ



Протокол №10 Ашымбаева Д.А.

от «24» августа 2017 г.

**ПОЛОЖЕНИЕ**

**об информационной безопасности.**

**1. Общие положении**

1.1. Информационная безопасность является одним из составных элементов

комплексной безопасности

1.2. Данное положение разработано в соответствии с Трудовым кодексом КР

"Об информации, информационных технологиях и о защите информации".

1.3. Под информационной безопасностью школы следует понимать состояние

защищенности информационных ресурсов, технологий их формирования и

использования, а также прав субъектов информационной деятельности.

Система информационной безопасности направлена на предупреждение угроз,

их своевременное выявление, обнаружение, локализацию и ликвидацию.

1.4. К объектам информационной безопасности в школе относятся:

• информационные ресурсы, содержащие документированную информацию, в

соответствии с перечнем сведений конфиденциального характера:

• информацию, защита которой предусмотрена законодательными актами КР. вт.ч. персональные данные:

• средства и системы информатизации, программные средства,

автоматизированные системы управления, системы связи и передачи данных,

осуществляющие прием, обработку, хранение и передачу информации с ограниченнымдоступом.

1.5. Система информационной безопасности (далее - СИБ) должна обязательнообеспечивать:

• конфиденциальность (защиту информации от несанкционированного раскрытияили перехвата);

• целостность (точность и полноту информации и компьютерных программ);

• доступность (возможность получения пользователями информации в пределахих компетенции).

1.6 Обеспечение информационной безопасности осуществляется по следующимнаправлениям:

• правовая зашита - это специальные законы, другие нормативные акты, правила,процедуры и мероприятия, обеспечивающие защиту информации на правовой основе:

• организационная зашита - это регламентация производственной деятельности и

взаимоотношений исполнителей на нормативно-правовой основе, исключающая или

ослабляющая нанесение какого-либо ущерба:

• 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 сведенийконфиденциального характера, персональных данных обучающихся, работников школы,требовать от своих сотрудников обеспечения сохранности и защиты этих сведений отвнешних и внутренних угроз.

2.2. Школа обязана обеспечить сохранность конфиденциальной информации.

2.3. Администрация школы:

• назначает ответственного за обеспечение информационной безопасности;

• издаёт нормативные и распорядительные документы, определяющие порядоквыделения сведений конфиденциального характера и механизмы их защиты;

• имеет право включать требования по обеспечению информационной

безопасности в коллективный договор;

• имеет право включать требования по защите информации в договоры по всемвидам деятельности;

• разрабатывает перечень сведений конфиденциального характера;

• имеет право требовать защиты интересов школы со стороны государственных исудебных инстанций.

2.4. Организационные и функциональные документы по обеспечениюинформационной безопасности:

• приказ директора школы о назначении ответственного за обеспечениеинформационной безопасности;

• должностные обязанности ответственного за обеспечение информационнойбезопасности;

• перечень защищаемых информационных ресурсов и баз данных;

• инструкция, определяющая порядок предоставления информации сторонниморганизациям по их запросам, а также по правам доступа к ней сотрудников школы и др.

2.5. порядок допуска сотрудников школы к информации предусматривает:

• принятие работником обязательств о неразглашении доверенных ему сведенийконфиденциального характера;

• ознакомление работника с нормами законодательства КР и школы обинформационной безопасности и ответственности за разглашение информацииконфиденциального характера;

• инструктаж работника специалистом по информационной безопасности;

• контроль работника ответственным за информационную безопасность при

работе с информацией конфиденциального характера.

3. Мероприятия по обеспечению информационной безопасности

Для обеспечения информационной безопасности в школе требуется проведениеследующих первоочередных мероприятий:

• защита интеллектуальной собственности школы;

• защита компьютерови подключения к системеИнтернета;

• организация защиты конфиденциальной информации, в т. ч. персональных

данных работников и обучающихся школы;

• учет всех носителей конфиденциальной информации.

4. Организация работы с информационными ресурсами и технологиями

4.1. Система организации делопроизводства:

• учет всей документации школы, в т. ч. и на электронных носителях, склассификацией по сфере применения, дате, содержанию;

• регистрация и учет всех входящих (исходящих) документов школы вспециальном журнале информации о дате получения (отправления) документа, откудапоступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);

• регистрация документов, с которых делаются копии, в специальном журнале(дата копирования, количество копий, для кого или с какой целью производитсякопирование);

• особый режим уничтожения документов.

4.2. В ходе использования, передачи, копирования и исполнения документов такженеобходимо соблюдать определенные правила:

4.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись вжурнале учета документов.

4.2.2. Документы, дела и издания с грифом "Для служебного пользования"

("Ограниченного пользования") должны храниться в служебных помещениях в надежнозапираемых и опечатываемых шкафах. При этом должны быть созданы условия,обеспечивающие их физическую сохранность.

4.2.3. Выданные для работы дела и документы с грифом "Для служебногопользования" ("Ограниченного пользования") подлежат возврату в канцелярию в тот же день.

4.2.4. Передача документов исполнителю производится только через ответственногоза организацию делопроизводства.

4.2.5. Запрещается выносить документы с грифом "Для служебного пользования" запределы школы.

4.2.6. При смене работников, ответственных за учет и хранение документов, дел иизданий, составляется по произвольной форме акт приема-передачи документов.

4.3.Для организации делопроизводства приказом директора школы назначаетсяответственное лицо. Делопроизводство ведется на основании инструкции поорганизации делопроизводства, утвержденной директором школы. Контроль запорядком его ведения возлагается на ответственного за информационнуюбезопасность.

5. Обеспечение безопасности в Школьном портале

5.1. Школьный портал относится к группе многопользовательских информационных систем сразными правами доступа. С учетом особенностей обрабатываемой информации, системасоответствует требованиям, предъявляемым действующим в Российской Федерациизаконодательством, к информационным системам, осуществляющим обработку персональныхданных.Школьный портал обеспечивает возможность защиты информации от потери инесанкционированного доступа на этапах её передачи и хранения.Для настройки прав пользователей в системе созданы отдельные роли пользователей сназначением разрешений на выполнение отдельных функций и ограничений по доступу кинформации, обрабатываемой в Школьном портале.

5.2.1.Участники образовательного процесса, имеющие доступ к Школьному порталу, неимеют права передавать персональные логины и пароли для входа на Школьный портал другим лицам.Передача персонального логина и пароля для входа в Школьный портал другим лицам влечет засобой ответственность в соответствии с законодательством Кыргызской Республики о защитеперсональных данных.

5.2.2.Участники образовательного процесса, имеющие доступ к Школьному порталу,соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль).

5.2.3.Участники образовательного процесса, имеющие доступ к Школьному порталу, в случаенарушения конфиденциальности условий доступа в личный кабинет, уведомляют в течение неболее чем одного рабочего дня со дня получения информации о таком нарушениируководителя ОО, службу технической поддержки Школьного портала.

5.2.4.Все операции, произведенные участниками образовательного процесса, имеющимидоступ к Школьному порталу, с момента получения информации руководителем ОО и службойтехнической поддержки о нарушении, указанном в предыдущем абзаце, признаютсянедействительными.

5.2.5.При проведении работ по обеспечению безопасности информации в Школьномпортале участники образовательного процесса, имеющие доступ к Школьному порталу, обязанысоблюдать требования законодательства Кыргызской Республики в области защиты персональныхданных