Министерство просвещения и науки Кабардино-Балкарской Республики
Государственное бюджетное общеобразовательное учреждение
«Санаторно-лесная школа»

Принято	**Согласовано**	**Утверждено**
на заседании Педагогического совета ГБОУ СЛШ протокол № 3 от 11 января 2023г.	с Советом родителей Протокол № 3 от 12 января 2023г	Приказом № 13 от 12 января 2023г Директор ГБОУ СЛШ ________ Джаппуева Л.Х.

ПОЛОЖЕНИЕ
об информационной безопасности ГБОУ «Санаторно-лесная школа» Минпросвещения КБР

1. Общие положения

1.1. Настоящее положение разработано в соответствии с

- Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.),
- Федеральный законом от 07.07.2003 № 126-ФЗ «О связи»,
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации"»,
- Федеральным законом от 27.07.2006 № 152-ФЗ (в ред. От 27.07.2011) «О персональных данных», Федеральным законом от 28.12.2010 № 390-ФЗ «О безопасности»,
- Федеральным законом от 29.12.2010г. №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»

1.2. Информационная безопасность является одним из составных элементов комплексной безопасности. Под информационной безопасностью ГБОУ «Санаторно-лесная школа» (далее – Учреждения) 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.

1.3. К объектам информационной безопасности в Учреждении относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
- информация, защита которой предусмотрена законодательными актами РФ, в т. 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 ограниченным доступом.

1.4. К информации, причиняющей вред здоровью и (или) развитию обучающихся, относится информация:

запрещенная для распространения среди обучающихся; распространение которой среди обучающихся определенных возрастных категорий ограничено.

1.4.1. К информации, запрещенной для распространения среди обучающихся, относится информация: побуждающая обучающихся к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству; способная вызвать у обучающихся желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством; обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Положением; отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи; оправдывающая противоправное поведение; содержащая нецензурную брань; содержащая информацию порнографического характера; о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

1.4.2. К информации, распространение которой среди обучающихся определенных возрастных категорий ограничено, относится информация: представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия; вызывающая у обучающихся страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания. самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий; представляемая в виде изображения или описания половых отношений между мужчиной и женщиной; содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

1.4. Система информационной безопасности должна обязательно обеспечивать:

– конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
– целостность (точность и полноту информации и компьютерных программ);
– доступность (возможность получения пользователями информации в пределах их компетенции)

- Ограничение детей от информации, наносящей вред здоровью и психическому здоровью

1.5. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая защита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита - это регламентация деятельности Учреждения 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, а так же вреда здоровью и развитию детей

2. Цели и задачи обеспечения безопасности информации

2.1. Главной целью обеспечения безопасности информации, циркулирующей в Учреждении, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа (далее по тексту - конфиденциальной или защищаемой информации) и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационной среды Учреждения.

2.2. Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в Учреждении;
- предотвращение нарушений прав личности обучающихся, работников Учреждения на сохранение конфиденциальности информации;
- предотвращение несанкционированных действий по блокированию информации.

2.3. Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;
- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам Учреждения, нарушению нормального функционирования и развития Учреждения;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;
- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;

- развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;
- развитие и совершенствование защищенного юридически значимого электронного документооборота;
- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности;
- создание механизмов управления системой информационной безопасности.

3. Правовые нормы обеспечения информационной безопасности

3.1. Учреждение имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников Учреждения, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

3.2. Учреждение обязано обеспечить сохранность конфиденциальной информации.

3.3. Администрация Учреждения:

- назначает ответственного за обеспечение информационной безопасности;
- имеет право включать требования по обеспечению информационной безопасности в коллективный договор;
- имеет право включать требования по защите информации в договоры по всем видам деятельности;
- разрабатывает перечень сведений конфиденциального характера;
- имеет право требовать защиты интересов Учреждения со стороны государственных и судебных инстанций.

3.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора Учреждения о назначении ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных;
- инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников Учреждения и др.

3.5. Порядок допуска сотрудников Учреждения к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства РФ и Учреждения об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
- инструктаж работника специалистом по информационной безопасности;

- контроль работника ответственным за информационную безопасность, при работе с
- информацией конфиденциального характера.

4. Организация системы обеспечения информационной безопасности

4.1. В целях реализации стоящих перед системой обеспечения информационной безопасности задач в Учреждении устанавливаются:

- защита интеллектуальной собственности Учреждения;
- защита компьютеров, локальных сетей и сети подключения к системе Интернета;
- организация защиты конфиденциальной информации, в т. ч. Персональных данных работников и обучающихся Учреждения;
- учет всех носителей конфиденциальной информации;
- контроль за использованием электронных средств информационного обеспечения деятельности Учреждения по прямому назначению;
- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности Учреждения нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;
- принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;
- обучение персонала Учреждения по вопросам обеспечения информационной безопасности;
- контроль за правильностью использования имеющихся в Учреждении средств телефонной и радиосвязи.

5. Организация работы с информационными ресурсами и технологиями

5.1. Для организации делопроизводства приказом директора Учреждения назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором Учреждения. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

5.2. Система организации делопроизводства:

- учет всей документации Учреждения, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов Учреждения в специальном журнале информации о дате получения (отправления) документа, откуда поступил 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 производится копирование);
- особый режим уничтожения документов.

5.3. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

5.3.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

5.3.2. Документы, дела и издания с грифом «Для служебного пользования» («Ограниченного пользования») должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

5.3.3. Выданные для работы дела и документы с грифом «Для служебного пользования» («Ограниченного пользования») подлежат возврату в канцелярию в тот же день.

5.3.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.

5.3.5. Запрещается выносить документы с грифом «Для служебного пользования» за пределы Учреждения.

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

5.4. Всѐ программное обеспечение устанавливается только с разрешения ответственного за информационную безопасность.

5. Меры по обеспечению защиты обучающихся от информации, причиняющей вред их здоровью и развитию

5.1. Ознакомление работников, в трудовые обязанности которых входит организация и осуществление оборота информационной продукции, запрещенной для обучающихся, с положениями законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, с локальными нормативными актами Учреждения, изданными в соответствии с законодательными и нормативными правовыми актами в указанной сфере.

5.2. Назначение работника, из числа АУП, ответственного за применение административных и организационных мер защиты обучающихся от информации, причиняющей вред их здоровью и (или) развитию, учитывающих специфику оборота информационной продукции, запрещенной для обучающихся, и за проверку порядка их применения.

5.3. Размещение на информационных стендах в местах, доступных для обучающихся, а также доведение иным доступным способом до третьих лиц сведений об изданных на основании Федерального закона локальных нормативных актах Учреждения

5.4. Размещение на официальном сайте Учреждения в сети «Интернет» информационной продукции, запрещенной для обучающихся, локальных нормативных актов, изданных на основании Федерального закона, а также сведений о применении административных и организационных мер, и обеспечение возможности свободного доступа к указанным документам.

5.5. Контроль за соответствием содержания и художественного оформления печатных изданий, полиграфической продукции (в том числе тетрадей, обложек для книг, закладок для книг), включая выдаваемую обучающимся в библиотеке художественную, научную и научно-популярную литературу, возрастным особенностям обучающихся, осуществляется работником библиотеки Учреждения.

5.5.1. При заказе литературы и периодических изданий работник библиотеки обращают внимание на наличие знака информационной продукции, устанавливаемого производителем.

5.5.2. В отсутствие указанного знака в установленном порядке осуществляется классификация информационной продукции.

5.6. Контроль за соответствием содержания сценариев, тематических вечеров и других зрелищных массовых мероприятий, используемых при их проведении эпизодов из художественных фильмов, телепрограмм и т.п. требованиям, предъявляемым к информационной продукции для обучающихся соответствующей возрастной группы осуществляется уполномоченными работниками подразделений Учреждения, ответственных за работу с детьми.

5.7. Во время учебного занятия (урока) в рамках учебного плана, доступ обучающихся к сети Интернет осуществляется по заявке лица, ответственного за проведение занятия. Контроль использования обучающимися сети Интернет осуществляет педагогический работник, ведущий занятие. При этом педагогический работник: наблюдает за целевым использованием компьютера и сети Интернет обучающимися; запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения обучающимся требований настоящего Положения и иных нормативных документов, регламентирующих использование сети Интернет в Учреждения; принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.