

**ПОЛОЖЕНИЕ**  
**о защите персональных данных и конфиденциальной информации**  
**ГБУ ДО СО «СШОРСЕ Ахмерова»**

**1. Общие положения.**

- 1.1. Положение о защите персональных данных и конфиденциальной информации (далее — Положение) разработано с целью защиты интересов ГБУ ДО СО «Спортивная школа олимпийского резерва по спортивным единоборствам имени С.Р.Ахмерова» на случай раскрытия (передачи) информации, которая не предназначена для широкого распространения.
- 1.2. Перечень сведений, которые относятся к конфиденциальной информации указан в приложении № 1 к данному Положению.
- 1.3. Положение определяет общий порядок обращения в Учреждении с документами на различных носителях, в том числе и электронными документами и сообщениями (далее— документами), содержащими конфиденциальную информацию.
- 1.4. Данное положение разработано на основе законодательных и нормативных актов Российской Федерации: Трудового кодекса Российской Федерации, Гражданского кодекса Российской Федерации, Уголовного кодекса Российской Федерации, ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Указа Президента РФ от 06.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера», ФЗ от 19.12.2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», ФЗ от 27.07.2006 г. № 152-ФЗ «О персональных данных».

1.5. В Положении употребляются следующие термины и определения:

- информация — сведения (сообщения, данные) независимо от формы их представления;
- информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
- обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешить или ограничивать доступ к информации, определяемой по каким-либо признакам;
- доступ к информации — возможность получения информации и ее использования;
- конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
- распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

- электронное сообщение — информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
- документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
- электронный документ — документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием ЭВМ, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;
- оператор информационной системы — граждане или юридические лица, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базе данных;
- сведения, относящиеся к конфиденциальной информации:
  - служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна);
  - сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (тайна переписки, телефонных переговоров, почтовых отправлений и др.);

#### 1.6. Не могут быть отнесены к конфиденциальной информации:

- акты законодательства, устанавливающие правовой статус государственных органов, организаций, учреждений, а также их права, свободы и обязанности граждан, порядок их реализации;
- сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая гидрометеорологическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасности всех работников и обучающихся в Учреждении;
- описание структуры учреждения, ее функций, направлений и форм деятельности;
- порядок рассмотрения и разрешения обращений граждан и юридических лиц, а также решения, принятые в ходе их рассмотрения;
- общедоступная информация;
- содержащихся в учредительных документах Учреждения документах, подтверждающих факт внесения записей о юридических лицах в соответствующие государственные реестры;
- о составе имущества государственного учреждения и об использовании им средств соответствующего бюджета;
- о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно - эпидемиологической и радиационной обстановке и других факторов, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и населения в целом;
- о численности, составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, о наличии свободных рабочих мест;
- о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;
- о нарушении законодательства РФ и фактах привлечения к ответственности за совершение этих нарушений;
- о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
- обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

1.7. На документах, содержащих конфиденциальную информацию, могут проставляться пометки **КОНФИДЕНЦИАЛЬНО**, **СТРОГО КОНФИДЕНЦИАЛЬНО**.

1.8. Директор Учреждения в пределах своей компетенции определяет:

- категории работников учреждения, уполномоченных относить информацию к разряду конфиденциальной и определять уровень доступа к такой информации;
- порядок передачи конфиденциальной информации другим организациям;
- организацию защиты конфиденциальной информации.

1.9. Не разрешается разглашать (распространять) конфиденциальную информацию, указанную в п.1.2. устно, письменно, путем демонстрации или передачи кому-либо соответствующих документов.

1.10. За разглашение конфиденциальной информации работник учреждения может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

## **2. Особенности работы с конфиденциальными документами.**

2.1. Необходимость проставления на документах пометок **КОНФИДЕНЦИАЛЬНО, СТРОГО КОНФИДЕНЦИАЛЬНО** определяется должностным лицом, подписывающим или утверждающим документ.

2.2. Должностные лица несут персональную ответственность за принятое решение.

2.3. Пометка **КОНФИДЕНЦИАЛЬНО, СТРОГО КОНФИДЕНЦИАЛЬНО** проставляется в правом верхнем углу документа.

2.4. Исполненные документы с пометкой **КОНФИДЕНЦИАЛЬНО, СТРОГО КОНФИДЕНЦИАЛЬНО** группируются в дела в соответствии с номенклатурой конфиденциальных дел.

2.5. Все имеющиеся документы, дела и издания, содержащие конфиденциальную информацию, должны храниться в служебных помещениях, в надежно запираемых шкафах или сейфах. Помещения должны отвечать требованиям режима, обеспечивающего физическую сохранность находящихся в них документации.

2.6. Запрещается оставлять на рабочих местах без присмотра или в незапертых шкафах (сейфах) конфиденциальные документы в течение рабочего дня или по его окончании.

2.7. Доступ посторонних лиц в помещения, предназначенные для работы с конфиденциальной информацией, по возможности, ограничивается.

2.8. К работе с конфиденциальными документами допускаются лица, способные по личным и деловым качествам обеспечить их сохранность, и только после оформления письменного обязательства о неразглашении сведений конфиденциального характера.

2.9. При выявлении нарушения требований порядка обращения с конфиденциальной информацией к лицу, допустившему нарушение, могут быть применены меры дисциплинарного взыскания вплоть до увольнения.

## **3. Обязанности работников, работающих с конфиденциальными сведениями, и их ответственность за разглашение данных сведений.**

3.1. Работники Учреждения, допущенные к конфиденциальным сведениям, несут ответственность за точное выполнение требований, предъявляемых к ним в целях обеспечения сохранности указанных сведений. До получения доступа к работе, связанной с конфиденциальными сведениями, им необходимо изучить настоящее Положение .

3.2. Работники, допущенные к работе с конфиденциальными сведениями, должны:

- не разглашать конфиденциальные сведения, ставшие им известными. В случае утечки подобных сведений, а также об утрате документов сообщить руководителю Учреждения;
- предъявлять для проверки по требованию руководства все числящиеся за ними документы, содержащие конфиденциальные сведения, а в случае нарушения установленных правил работы с ними предоставлять соответствующие объяснения;

- знакомиться только с теми документами и выполнять только те работы, к которым они допущены;
- строго соблюдать правила пользования документами, содержащими конфиденциальные сведения;
- выполнять требования, исключающие возможность ознакомления с конфиденциальными сведениями посторонних лиц, включая работников Учреждения, не имеющих к указанным документам прямого отношения;
- исключить использование конфиденциальных сведений в своих личных интересах, в интересах третьих лиц, а также в интересах других организаций.

3.3. Ответственность за разглашение сведений, ограниченного распространения и утрату документов, содержащих такие сведения, устанавливается в соответствии с действующим законодательством Российской Федерации.

**ПЕРЕЧЕНЬ**  
**сведений конфиденциального характера**

1. Персональные данные работников Учреждения, а также обучающихся в Учреждении.
2. Сведения об экономической эффективности, финансовой деятельности Учреждения и распределении финансов.
3. Сведения о состоянии компьютерного обеспечения.
4. Сведения о содержании программного обеспечения.
5. Фактическое состояние расчетов с контрагентами.
6. Условия предлагаемых, осуществляемых и исполненных договоров, платежей.
7. Сведения о порядке и состоянии организации охраны, системе сигнализации, паролях.
8. Сведения об информационной системе Учреждения и применяемых способах информационной защиты.