ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «СТАВРОПОЛЬСКИЙ КРАЕВОЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ, ПОВЫШЕНИЯ КВАЛИФИКАЦИИ И ПЕРЕПОДГОТОВКИ РАБОТНИКОВ ОБРАЗОВАНИЯ»

# ПРИКАЗ

«12» мая 2017 г. №173/1 о/д

г. Ставрополь

Об организации работы
с персональными данными

В соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановлений Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки персональных данных в институте проректора по информатизации и региональному развитию системы образования (Устименко Т.А.).
2. Назначить ответственным за выполнение работ по обеспечению безопасности персональных данных в институте начальника материально – технического обеспечения (Дорохин С.С.).
3. Возложить функции администратора сети на инженера отдела материально-технического обеспечения (Скрыник И.А.).
4. Утвердить:
4.1. Правила обработки персональных данных в государственном бюджетном учреждении дополнительного профессионального образования «Ставропольский краевой институт развития образования, повышения квалификации и переподготовки работников образования» (далее - институт) (Приложение № 1).
4.2. Положение по обработке и защите персональных данных обучающихся (слушателей) института (Приложение № 2).
4.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним локальными нормативными актами института (Приложение № 3).

4.4. Порядок доступа работников института в помещения, в которых ведется обработка персональных данных (Приложение № 4).

4.5. Инструкцию по организации парольной защиты в институте (Приложение № 5).

4.6. Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (Приложение № 6).

4.7. Типовую форму согласия на обработку персональных данных в институте иных субъектов персональных данных (Приложение № 7).

4.8. Типовое обязательство работника института, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним эффективного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (Приложение № 8).

4.9. Перечни информационных систем персональных данных (Приложение № 9).

4.10. Перечень должностей работников института, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (Приложение 10).

4.11. Перечень программного обеспечения, разрешенного к использованию в институте (Приложение 11).

4.12. Перечни персональных данных, обрабатываемых в институте (Приложение 12).

4.13. Должностную инструкцию ответственного за организацию обработки персональных данных в институте (Приложение 13).

4.15. Должностную инструкцию администратора сети (Приложение 14).

5. Отделу кадрового и правового обеспечения (Саблиной С.Н.) довести настоящий приказ до сведения сотрудников, в части их касающейся.

6. Контроль за исполнением настоящего приказа оставляю за собой.

7. Настоящий приказ вступает в силу со дня его подписания.

Ректор Е.В. Евмененко

Приложение № 1
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

# ПРАВИЛА
# ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
# В ИНСТИТУТЕ

## I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Правила обработки персональных данных (далее - Правила) устанавливают единый порядок обработки персональных данных в государственном бюджетном учреждении дополнительного профессионального образования «Ставропольский краевой институт развития образования, повышения квалификации и переподготовки работников образования» (далее - институт).

2. Обработка персональных данных в институте осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ), настоящими Правилами и другими нормативными правовыми актами, касающимися обработки персональных данных.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в том же значении, что и в Федеральном законе № 152-ФЗ.

4. Целью настоящих Правил является обеспечение защиты персональных данных граждан от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5. Настоящие Правила устанавливают и определяют:

1) процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;

2) цели обработки персональных данных;

3) содержание обрабатываемых персональных данных для каждой цели обработки персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) сроки обработки и хранения обрабатываемых персональных данных;

6) порядок уничтожения обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований;

6. Основные условия обработки персональных данных:

6.1. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных даных, а именно:

после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных подпунктами 2 - 7, 9 - 11 пункта 1 статьи 6 Федерального закона № 152-ФЗ;

после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Ставропольскому краю, за исключением случаев, предусмотренных пунктом 2 статьи 22 Федерального закона № 152-ФЗ.

6.2. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящими Правилами и подписывают обязательство о неразглашении информации в порядке, установленном в институте.

## II. ПРОЦЕДУРЫ, НАПРАВЛЕННЫЕ НА ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7. Меры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации:

7.1. Информационные ресурсы, содержащие персональные данные, созданные, приобретенные, накопленные в институте, а также полученные путем иных установленных законом способов, являются собственностью институте и не могут быть использованы иначе, как с разрешения ректора или в установленных законом случаях.

7.2. К мерам, направленным на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных относятся:

назначение ответственного за организацию обработки персональных данных в институте;

применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с пунктами 1 и 2 статьи 19 Федерального закона № 152-ФЗ;

осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

оценка вреда, который может быть причинен субъектам персональным данных в случае нарушения законодательства Российской Федерации и настоящих Правил;

ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных и настоящими Правилами;

запрет на обработку персональных данных лицами, не допущенными к их обработке;

запрет на обработку персональных данных под диктовку.

7.3. Документы, определяющие политику в отношении обработки персональных данных, подлежат обязательному опубликованию на официальном сайте института в течение 10 дней после их утверждения.

7.4. За разглашение информации, содержащей персональные данные, нарушение порядка обращения с документами и машинными носителями информации, содержащими такую информацию, а также за нарушение режима защиты, обработки и порядка использования этой информации, работник института может быть привлечен к дисциплинарной или иной ответственности, предусмотренной действующим законодательством.

8. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации:

8.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации института осуществляется в соответствии с требованиями законодательства Российской Федерации.

8.2. При эксплуатации автоматизированных информационных систем необходимо соблюдать следующие требования:

к работе допускаются только лица, назначенные соответствующим приказом;

на персональных электронных вычислительных машинах (далее - ПЭВМ), дисках, папках и файлах, на которых обрабатываются и хранятся сведения о персональных данных, должны быть установлены пароли (идентификаторы);

на период обработки защищаемой информации в помещении могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации;

допуск других лиц в указанный период может осуществляться с разрешения ректора или лица, отвечающего за защиту информации в институте.

8.3. Руководители подразделений института, работники института, осуществляющие обработку персональных данных (далее - пользователи) обязаны контролировать и выполнять предусмотренные в институте меры по защите информации, содержащей персональные данные.

8.4. Руководители структурных подразделений института обязаны:

участвовать в подготовке перечня персональных данных, обрабатываемых на ПЭВМ подразделения;

готовить к утверждению списки работников, которых по своим должностным обязанностям необходимо допустить к работе с персональными данными в информационной системе института;

контролировать целевое использование работниками ресурсов информационно-телекоммуникационной сети «Интернет»;

выборочно контролировать характер исходящей информации, направляемой пользователями по электронной почте другим адресатам и принимать оперативные меры к соблюдению ими установленных требований по защите персональных данных;

при обнаружении нарушений установленных требований по защите персональных данных, в результате которых вскрыты факты их разглашения, прекратить работы на рабочем месте, где обнаружены нарушения, доложить ректору и поставить в известность своего непосредственного начальника;

назначать служебные расследования по фактам разглашения информации, содержащей персональные данные, или утери документов, содержащих такую информацию, по фактам нарушений пользователями правил, установленных для работы с персональными данными в ЛВС, а также нарушений требований по защите информации;

обеспечивать условия для работы администратора сети при проверке в подразделении эффективности предусмотренных мер защиты информации;

определять порядок передачи информации, содержащей персональные данные, другим подразделениям института, сторонним организациям и органам.

8.5. При приеме на работу работник предупреждается об ответственности за разглашение сведений, содержащих персональные данные, которые станут ему известными в связи с предстоящим выполнением своих должностных обязанностей.

8.6. Пользователь обязан:

знать правила работы в локальной вычислительной сети (далее - ЛВС) и принятые меры по защите ресурсов ЛВС (в части, его касающейся);

при работе на своей рабочей станции (ПЭВМ) и в ЛВС выполнять только служебные задания;

перед началом работы на ПЭВМ проверить свои рабочие папки на жестком магнитном диске, съемные магнитные носители информации на отсутствие вирусов с помощью штатных средств антивирусной защиты, убедиться в исправности своей рабочей станции;

при сообщениях о появлении вирусов немедленно прекратить работу, доложить администратору сети, своему непосредственному начальнику;

при обработке информации, содержащей персональные данные, использовать только зарегистрированные в журналах учета института машинные носители информации (далее - МНИ);

при необходимости использования машинных носителей, поступивших из других подразделений, учреждений, предприятий и организаций, прежде всего, провести проверку этих носителей на отсутствие вирусов;

выполнять предписания администратора сети и ответственного за защиту информации в институте (работников сектора программно-информационного обеспечения);

представлять для контроля свою рабочую станцию (ПЭВМ) руководителю подразделения, администратору сети и специалисту сектора программно-информационного обеспечения;

сохранять в тайне свой индивидуальный пароль, периодически, но не реже чем один раз в полгода, изменять его и не сообщать другим лицам;

вводить пароль и другие учетные данные, убедившись, что клавиатура находится вне поля зрения других лиц;

при обнаружении различных неисправностей в работе компьютерной техники или ЛВС, недокументированных свойств в программном обеспечении, нарушений целостности пломб (наклеек, печатей), несоответствии номеров на аппаратных средствах сообщить администратору сети и поставить в

известность руководителя подразделения. Пользователю при работе запрещается:

играть в компьютерные игры;

приносить различные компьютерные программы и пытаться установить их на локальный диск компьютера без уведомления администратора сети;

перенастраивать программное обеспечение компьютера;

самостоятельно вскрывать комплектующие рабочей станции (ПЭВМ);

запускать на своей рабочей станции (ПЭВМ) или другой рабочей станции сети любые системные или прикладные программы, кроме установленных администратором сети;

изменять или копировать файл, принадлежащий другому пользователю, не получив предварительно разрешения владельца файла;

оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации (при наличии), машинные носители и распечатки, содержащие персональные данные;

допускать к подключенной в сеть рабочей станции (ПЭВМ) посторонних лиц;

производить копирование для временного хранения информации, содержащей персональные данные, на неучтенные носители;

работать на рабочей станции (ПЭВМ) в сети с информацией, содержащей персональные данные, при обнаружении неисправностей станции (ПЭВМ), влияющих на защиту информации;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты информации, которые могут привести к утечке, блокированию, искажению или утере информации, содержащей персональные данные;

отсылать по электронной почте информацию для решения личных проблем, а также информацию по просьбе третьих лиц без согласования с руководством подразделения;

запрашивать и получать из информационно-телекоммуникационной сети «Интернет» материалы развлекательного характера (игры, клипы и т.д.);

запрашивать и получать из информационно-телекоммуникационной сети «Интернет» программные продукты, кроме случаев, связанных со служебной необходимостью. При этом необходимо согласование с руководителем своего подразделения и обеспечение процесса администратором сети.

8.7. Работники не могут использовать в личных целях персональные данные, ставшие известными им вследствие выполнения должностных обязанностей.

9. Порядок обработки персональных данных без использования средств автоматизации ведется в соответствии с требованиями постановления Правительства Российской Федерации № 687 от 15 сентября 2008 года:

9.1. Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка персональных

данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

9.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

9.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;

персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

9.4. При использовании типовых форм документов характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных (при необходимости получения письменного согласия на обработку персональных данных);

типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

9.5. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

9.6. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с

сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

9.7. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных - осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

при необходимости уничтожения или блокирования части персональных данных - уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

9.8. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

9.9. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ.

9.10. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в раз личных целях.

## III. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

10. Целью обработки персональных данных является содействия субъектам персональных данных в осуществлении учебной, научной, трудовой деятельности, обеспечения личной безопасности, учета результатов исполнения договорных обязательств, а также наиболее полного исполнения институтом обязательств и компетенций в соответствии с законодательством Российской Федерации, Уставом института.

## IV. СОДЕРЖАНИЕ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

11. К персональным данным, обрабатываемым для достижения целей, указанных в пункте 10 настоящих Правил относятся:

1) анкетные и биографические данные гражданина, включая адрес места жительства и проживания;

2) паспортные данные или данные иного документа, удостоверяющего личность и гражданство (включая серию, номер, дату выдачи, наименование органа, выдавшего документ);

3) сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (включая серию, номер, дату выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, дату начала и завершения обучения);

4) сведения о трудовой деятельности, опыте работы, занимаемой должности, трудовом стаже, повышении квалификации и переподготовках;

5) сведения о номере, серии, дате выдачи трудовой книжки (вкладыша в нее) и записях в ней, содержание и реквизиты трудового договора (контракта);

6) сведения о составе семьи и наличии иждивенцев;

7) сведения о месте работы или учебы членов семьи;

8) сведения о состоянии здоровья и наличии заболеваний (когда это необходимо в случаях, установленных законом);

9) сведения об отношении к воинской обязанности;

10) сведения о доходах и обязательствах имущественного характера, в том числе членов семьи;

11) сведения об идентификационном номере налогоплательщика;

12) сведения о социальных льготах и о социальном статусе;

13) сведения из страховых полисов обязательного (добровольного) медицинского страхования;

14) сведения о номере и серии страхового свидетельства государственного пенсионного страхования;

15) изображение;

16) номер телефона, факса, адрес электронной почты.

## V. КАТЕГОРИИ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ

13. К субъектам, персональные данные которых обрабатываются, относятся:

1) работники института, а также члены их семей;

2) обучающиеся (слушатели) института;

3) лица, состоящие с институтом в гражданско-правовых отношениях;

4) кандидаты на замещение вакантных должностей;

5) граждане, обратившиеся в институт (жалоба, заявление, предложение, запрос и т.п.).

## VI. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ОБРАБАТЫВАЕМЫХ

ПЕРСОНАЛЬНЫХ ДАННЫХ

14. Сроки обработки и хранения персональных данных определяются:

1) Приказом Минкультуры Российской Федерации от 25 августа 2010 г. № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»;

2) сроком исковой давности;

3) иными требованиями законодательства Российской Федерации, нормативными правовыми актами Ставропольского края, нормативными правовыми актами института.

15. Особенности хранения персональных данных:

Если срок хранения персональных данных не установлен законодательством Российской Федерации, нормативными правовыми актами Ставропольского края, нормативными правовыми актами института или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, то хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

## VII. ПОРЯДОК УНИЧТОЖЕНИЯ ОБРАБОТАННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

16. Под уничтожением обработанных персональных данных понимаются действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных, или в результате которых уничтожаются материальные носители персональных данных.

17. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

18. Порядок уничтожения обработанных персональных данных:

Уничтожению подлежат утратившие практическое значение и не имеющие исторической или иной ценности носители информации, содержащие персональные данные. При уничтожении таких носителей должно быть исключено ознакомление с ними посторонних лиц, неполное или случайное их уничтожение.

Уничтожение производится путем сожжения, расплавления, дробления, растворения, химического разложения или превращения в мягкую бесформенную массу или порошок. Допускается уничтожение документов путем измельчения в бумажную сечку. Магнитные и фотографические носители уничтожаются сожжением, дроблением, расплавлением и другими способами, исключающими возможность их восстановления.

Уничтожение обработанных персональных данных производится комиссионно, с составлением соответствующего акта. Состав комиссии назначается приказом ректора сроком на 1 год. В комиссию назначаются лица, допущенные к работе с персональными данными.

На документальные материалы, отобранные комиссией для уничтожения, составляется акт об уничтожении документов, который подписывается членами комиссии и утверждается ректором.

Отобранные и включенные в акт об уничтожении документальные материалы после их сверки членами комиссии хранятся отдельно от других материалов.

Уничтожение должно производиться в возможно короткий срок после утверждения ректором акта об уничтожении документов.

19. Без оформления акта уничтожаются: испорченные бумажные и технические носители, черновики и проекты документов и другие материалы, образовавшиеся при исполнении документов, содержащих персональные данные.

В процедуру уничтожения документов и носителей информации без составления акта входит проведение следующих мероприятий:

разрывание листов, разрушение магнитного или иного технического носителя в присутствии исполнителя и руководителя подразделения, допущенных к обработке персональных данных;

накапливание остатков носителей в опечатываемом ящике (урне); физическое уничтожение остатков носителей несколькими сотрудниками подразделения, допущенными к работе с персональными данными;

внесение отметок об уничтожении в учетные формы документов и носителей.

Приложение № 2
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

# ПОЛОЖЕНИЕ
# ПО ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБУЧАЮЩИХСЯ (СЛУШАТЕЛЕ) ИНСТИТУТА

1. Настоящие Положение по обработке и защите персональных данных обучающихся (слушателей) института (далее - Положение) разработано на основании Конституции Российской Федерации, Федерального закона от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и постановления Правительства Российской Федерации от 17.11.11. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» с целью обеспечения уважения прав и основных свобод каждого слушателя и аттестующегося при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

## I. ОБЩИЕ ПОЛОЖЕНИЯ

2. Персональные данные слушателя и аттестующегося - сведения о фактах, событиях и обстоятельствах его жизни, позволяющие идентифицировать его личность, необходимые государственному бюджетному учреждению дополнительного профессионального образования «Ставропольский краевой институт развития образования, повышения квалификации и переподготовки работников образования» (далее - институт) в связи с оказанием образовательной услуги и касающиеся слушателей.

3. К персональным данным относятся:

1) сведения, содержащиеся в паспорте или и ном документе, удостоверяющем личность;

2) информация об успеваемости;

3) документ о месте проживания;

4) иные сведения, необходимые для качественного оказания образовательной услуги.

4. Институт может получить от заказчика образовательной услуги (работодателя слушателя/ аттестующегося) следующие данные о слушателях при условии получения Заказчиком согласия работников на передачу данных институту:

1) фамилии, имени, отчестве, дате рождения, месте жительства;

2) уровне образования, специальности;

3) копии документов о предыдущем образовании;

4) копию паспорта.

5. Иные персональные данные слушателя, необходимые в связи с оказанием образовательной услуги, институт может получить только с письменного согласия самого слушателя.

6. Персональные данные слушателя являются конфиденциальной информацией и не могут быть использованы администрацией или любым друг им лицом в личных целях.

7. При определении объёма и содержания персональных данных слушателя институт руководствуется Конституцией Российской Федерации, федеральными законами и настоящим Положением.

## II. ХРАНЕНИЕ, ОБРАБОТКА И ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ СЛУШАТЕЛЯ

8. Обработка персональных данных слушателя осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов в целях качественного оказания образовательной услуги.

9. Право доступа к персональным данным слушателя имеют:

1) Ректор;

2) Проректор;

3) Доцент (осуществляющий функции заведующего кафедрой);

4) Профессорско–преподавательский состав;

5) Специалист по учебно-методической работе;

6) Методист.

7) Начальник отдела планирования и организации учебной деятельности;

8) Начальник отдела аттестации педагогических работников;

9) Руководитель регионального центра обработки информации;

10. Права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных слушателя, определяются трудовыми договорами и должностными инструкциями.

## III. ОБЯЗАННОСТИ РАБОТНИКОВ ИНСТИТУТА, ИМЕЮЩИХ ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ СЛУШАТЕЛЯ

11. Работники института, имеющие доступ к персональным данным слушателя, обязаны:

1) не разглашать персональные данные обучающегося третьей стороне без письменного согласия слушателя кроме случаев, когда в соответствии с федеральными законами такого согласия не требуется;

2) использовать персональные данные слушателя, полученные только от него лично или от Заказчика образовательной услуги;

3) обеспечить защиту персональных данных слушателя, в порядке установленном законодательством Российской Федерации и локальными нормативными актами института;

4) соблюдать требование конфиденциальности персональных данных слушателя;

5) исключать или исправлять по письменному требованию слушателя его недостоверные или неполные персональные данные, а также данные, обработанные с нарушением требований законодательства Российской Федерации;

6) обеспечить слушателю свободный доступ к его персональным данным, включая право на получение копий любой записи, содержащей его персональные данные;

7) предоставить по требованию слушателя полную информацию о его персональных данных и обработке этих данных.

12. Лица, имеющие доступ к персональным данным слушателя, не вправе:

1) получать и обрабатывать персональным данным слушателя о его религиозных и иных убеждениях, семейной и личной жизни;

2) предоставлять персональные данные слушателя в коммерческих целях.

## IV. ПРАВА И ОБЯЗАННОСТИ СЛУШАТЕЛЯ, ЗАКАЗЧИКА ОБРАЗОВАТЕЛЬНОЙ УСЛУГИ

13. В целях обеспечения защиты персональных данных, хранящихся в институте, слушатель, заказчики образовательной услуги имеют право на:

1) требование об исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства;

2) требование об извещении всех лиц, которым ранее были сообщены неверные или неполные персональные данные слушателя, обо всех, произведенных в них исключениях, исправлениях или дополнениях.

## V. ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ СЛУШАТЕЛЯ

14. Персональные данные слушателя должны храниться в несгораемом, запирающемся шкафу на бумажных носителях и на электронных носителях с ограниченным доступом (имеющих средства защиты информации от несанкционированного доступа):

1) документы, поступившие от Заказчика образовательной услуги;

2) сведения, поступившие от слушателя;

3) иная информация, которая касается оказания образовательных услуг слушателю.

## VI. ОТВЕТСТВЕННОСТЬ

Защита прав слушателей, установленных законодательством Российской Федерации и настоящим Положением, осуществляется судом в целях пресечения неправомерного использования персональных данных слушателей, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных слушателя, привлекаются к дисциплинарной и материальной ответственности, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами

Приложение № 3
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

# ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, УСТАНОВЛЕННЫМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ «О ПЕРСОНАЛЬНЫХ ДАННЫХ», ПРИНЯТЫМИ В СООТВЕТСТВИИ С НИМ ЛОКАЛЬНЫМИ НОРМАТИВНЫМИ АКТАМИ ИНСТИТУТА

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним локальными нормативными актами института (далее - Правила) устанавливают порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном учреждении дополнительного профессионального образования «Ставропольский краевой институт развития образования, повышения квалификации и переподготовки работников образования» (далее - институт).

2. Осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в института осуществляется в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ), настоящими Правилами и другими нормативными правовыми актами, касающимися обработки персональных данных.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в том же значении, что и Федеральном законе № 152-ФЗ.

4. Целью осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - внутренний контроль) является обеспечение защиты персональных данных от несанкционированного доступа, неправомерного их использования или утраты, определение порядка и правил осуществления внутреннего контроля.

5. Внутренний контроль делится на текущий, плановый и внеплановый.

6. Текущий внутренний контроль осуществляется на постоянной основе ответственным за организацию обработки персональных данных в институте (далее - ответственный за организацию обработки) в ходе мероприятий по обработке персональных данных.

Ответственный за организацию обработки имеет право:

запрашивать у сотрудников института информацию, необходимую для реализации полномочий;

требовать от уполномоченных на обработку персональных данных

должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

вносить ректору предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

вносить ректору предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации о персональных данных.

7. Плановый внутренний контроль осуществляется комиссией, образуемой приказом ректора, в состав которой входят работники института, допущенные к обработке персональных данных.

Плановый внутренний контроль соответствия обработки персональных данных установленным требованиям в институте проводится на основании утвержденного ректором плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям, разрабатываемого председателем комиссии. Периодичность плановой проверки - не реже одного раза в год.

8. Внеплановый внутренний контроль может осуществляться на основании поступившего в институт письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется председателем комиссии в течение 3 рабочих дней с момента поступления соответствующего заявления.

В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в ее результатах.

9. При проведении внутреннего контроля ответственным за организацию обработки или комиссией должны быть полностью, объективно и всесторонне изучены:

наличие, учет, порядок хранения и обезличивания персональных данных;

порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;

порядоки условия применения средств защиты информации;

эффективность принимаемых мер по обеспечению безопасности персональных данных;

состояние учета ПЭВМ и съемных носителей информации, содержащей персональные данные;

соблюдение правил доступа к персональным данным;

наличие (отсутствие) фактов несанкционированного доступа к персональным данным;

порядок проведения мероприятий и результаты по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

порядок проведения мероприятий по обеспечению целостности персональных данных.

10. В отношении персональных данных, ставших известными членам комиссии или ответственному за организацию обработки в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

11. Срок проведения плановой и внеплановой проверки не может составлять более 30 дней со дня принятия решения о ее проведении.

12. Результаты внутреннего контроля оформляются в виде протокола проведения внутренней проверки (далее - протокол).

13. При выявлении в ходе внутреннего контроля нарушений ответственным за организацию обработки либо председателем комиссии в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

14. Протоколы хранятся у ответственного за организацию обработки в течение текущего года. Уничтожение протоколов проводится ответственным за организацию обработки самостоятельно в январе года, следующего за проверочным годом.

15. О результатах внутреннего контроля и мерах, необходимых для устранения нарушений, ректору докладывает ответственный за организацию обработки либо председатель комиссии.

Приложение № 4
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

# ПОРЯДОК
# ДОСТУПА РАБОТНИКОВ ИНСТИТУТА В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящий Порядок доступа работников института в помещения, в которых ведется обработка персональных данных (далее - Порядок), разработан в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и другими нормативными правовыми актами.

Целью настоящего Порядка является исключение несанкционированного доступа к персональным данным, обрабатываемым в государственном бюджетном учреждении дополнительного профессионального образования «Ставропольский краевой институт развития образования, повышения квалификации и переподготовки работников образования» (далее - институт), лиц, не допущенных к обработке персональных данных в институте.

Персональные данные относятся к конфиденциальной информации. Работники института, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе, установлением правил доступа в помещения, где обрабатываются персональные данные с использованием и без использования средств автоматизации.

Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. При хранении материальных носителей персональных данных, в том числе на бумажном носителе, должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

В помещения, где размещены технические средства, позволяющие

осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только работники института, допущенные к работе с ними.

Нахождение в помещениях, в которых ведется обработка персональных данных, лиц, не являющихся работниками института, или работников института, не допущенных к обработке персональных данных, возможно только в присутствии работника института, обрабатывающих в данном помещении персональные данные или допущенных к этим персональным данным. Время нахождения в помещениях ограничивается временем решения служебного вопроса, в рамках которого возникла необходимость пребывания в помещении. Все сотрудники, постоянно работающие в помещении, должны быть допущены к работе с соответствующими видами персональных данных.

Работники института, допущенные к работе с персональными данными, не должны покидать помещение не убедившись, что доступ посторонних лиц к персональным данным невозможен. Запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении.

Ответственные за организацию доступа в помещения института, в которых ведется обработка персональных данных, назначаются приказом.

Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, проводится в порядке, определенном Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним локальными нормативными актами института.

После окончания рабочего дня дверь каждого помещения, в котором ведется обработка персональных данных, закрывается на ключ и опечатывается, либо ставится на сигнализацию. Ключи в опечатанных тубусах сдаются дежурному охраннику.

В служебных помещениях, занимаемых институтом, применяются организационные, технические и физические меры, направленные для защиты от нецелевого использования, несанкционированного доступа, раскрытия, потери, изменения и уничтожения обрабатываемых персональных данных.

К указанным мерам относятся:

физические меры защиты: установка дверей, снабженных замками, сейфов, решеток, штор или жалюзи на окнах, расположение мониторов, уничтожение носителей, содержащих персональные данные, и т.д.;

технические меры защиты: применение антивирусных программ, программ защиты, установление паролей на персональных компьютерах, применение съемных носителей информации и т.д.;

организационные меры защиты: обучение и ознакомление с принципами безопасности и конфиденциальности, доведение до операторов обработки персональных данных важности защиты персональных данных и способов обеспечения защиты, допуск к обработке персональных данных только специально назначенных людей и т.д.

Приложение № 5
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

# ИНСТРУКЦИЯ
# ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ В ИНСТИТУТЕ

1.1. Первичный пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые администратором сети при создании новой учетной записи.

1.1.1. Установку первичного пароля производит администратор сети при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на системном администраторе.

1.1.2. Первичный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

1.1.3. При создании первичного пароля, администратор сети обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

1.1.4. Первичный пароль также используется при сбросе забытого пароля на учетную запись. В любом случае, при использовании первичного пароля все требования настоящего документа сохраняются.

1.2. Основной пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику организации, используемая для подтверждения подлинности владельца учетной записи.

1.2.1. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

1.2.3. Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам, в том числе сотрудникам отдела материально-технического обеспечения, записывать его, а также пересылать открытым текстом в электронных сообщениях.

1.2.4. Пользователь обязан не реже одного раза в месяц производить смену основного пароля соблюдая требования настоящего документа.

1.2.5. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом системному администратору и изменить основной пароль.

1.2.6. Восстановление забытого основного пароля пользователя осуществляется администратором сети путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной либо электронной заявки пользователя.

1.2.7. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

1.2.8. Для предотвращения угадывания паролей администратором сети обязан настроить механизм блокировки учетной записи при трехкратном

неправильном вводе пароля.

1.2.9. Разблокирование учетной записи пользователя осуществляется администратором сети на основании заявки владельца учетной записи (возможен вариант автоматического разблокирования через продолжительный промежуток времени).

1.3. Административный пароль - комбинация символом (буквы, цифры, знаки препинания, специальные символы), известная системному администратору (администратору БД, администратору приложения), используемая при настройке служебных учетных записей, учетных записей служб и сервисов, а также специальных учетных записей.

1.3.2. Администратор сети несет персональную ответственность за сохранение в тайне административного пароля. Запрещается сообщать пароль другим лицам, в том числе сотрудникам института, записывать его, а также пересылать открытым текстом в электронных сообщениях.

1.3.3. Администратор сети обязан не реже одного раза в месяц производить смену административного пароля, соблюдая требования настоящего документа.

1.3.4. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом администратору сети и изменить административный пароль.

Копии административных паролей должны храниться в опечатанном конверте в отделе материально-технического обеспечения.

Приложение № 6
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

ТИПОВАЯ ФОРМА
разъяснения субъекту персональных
данных юридических последствий отказа
предоставить свои персональные данные

Мне, _____,
(фамилия, имя, отчество)
разъяснены юридические последствия отказа предоставить свои персональные данные _____
_____.
(ГБУ ДПО «Ставропольский краевой институт развития образования, повышения квалификации и переподготовки работников образования»)

В соответствии с «Правилами обработки персональных данных в государственном бюджетном учреждении дополнительного профессионального образования «Ставропольский краевой институт развития образования, повышения квалификации и переподготовки работников образования», определен перечень персональных данных, которые субъект персональных данных обязан предоставить в связи с _____
_____
_____
_____
_____
(учебной, научной, трудовой деятельности, обеспечения личной безопасности, учета результатов исполнения договорных обязательств)

Я предупрежден, что в случае отказа предоставить свои персональные данные, (далее нужное подчеркнуть) государственному бюджетному учреждению дополнительного профессионального образования «Ставропольский краевой институт развития образования, повышения квалификации работников образования» в сфере деятельности мои права могут быть реализованы не в полном объеме; мои права на труд, на пенсионное обеспечение и медицинское страхование не могут быть реализованы в полном объеме, а трудовой договор подлежит расторжению.

«__» _____ 20__ г. _____/_____
(дата) (подпись) (расшифровка подписи)

Приложение № 7
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

ТИПОВАЯ ФОРМА
согласия на обработку персональных данных

Я, _____,
(фамилия, имя, отчество)
зарегистрированный по адресу: _____
_____,
паспорт серия _____ номер _____ выдан «__» _____ 20__ г.
(дата выдачи)
_____,
(наименование органа, выдавшего документ)
в соответствии со статьей 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» своей волей, в своем интересе и с целью решения вопросов сферы деятельности института, даю согласие

_____

(Государственное бюджетное учреждение дополнительного профессионального образования «Ставропольский краевой институт развития образования, повышения квалификации и переподготовки работников образования») (далее - оператору) на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение
персональных данных, а именно:

1) фамилия, имя, отчество;
2) дата рождения;
3) адрес регистрации по месту жительства;
4) адрес фактического проживания;
5) данные документа, удостоверяющего личность субъекта персональных данных;
6) почтовый адрес;
7) номер телефона, факса, адрес электронной почты;
8) индивидуальный налоговый номер;
9) номер страхового свидетельства обязательного пенсионного страхования;
10) реквизиты банковского счета;
11) данные о семейном положении;
12) данные на доверенное лицо;
13) сведения о социальных льготах и о социальном статусе.

Если мои персональные данные можно получить только у третьей стороны, то я должен быть уведомлен об этом заранее с указанием целей, предполагаемых источников и способов получения персональных данных. На это должно быть получено мое согласие.

Мне разъяснены мои права и обязанности, связанные с обработкой персональных данных, в том числе моя обязанность проинформировать оператора в случае изменения моих персональных данных и мое право в любое время отозвать свое согласие путем направления соответствующего письменного заявления оператору.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока до достижения цели обработки персональных данных или его отзыва мной в письменной форме.

«__» _____ 20__ г. _____/_____

(дата) (подпись) (расшифровка подписи)

Приложение № 8
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО
работника института, непосредственно
осуществляющего обработку персональных данных,
ставших известными ему в связи с исполнением
должностных обязанностей

Я, _____
(фамилия, имя, отчество)

_____

_____
(должность)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей в государственном бюджетном учреждении дополнительного профессионального образования «Ставропольский краевой институт развития образования, повышения квалификации и переподготовки работников образования» (далее - институт), в случае расторжения со мной договора, освобождения меня от замещаемой должности и увольнения.

В соответствии со статьей 7 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией. Я обязан(а) не раскрывать третьим лицам и не распространять персональные данные, ставшие известными мне в связи с исполнением должностных обязанностей в институте, без согласия субъекта персональных данных.

Ответственность, предусмотренная Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и другими федеральными законами, мне разъяснена.

«__» _____ 20__ г. _____/_____
(дата) (подпись) (расшифровка подписи)

Приложение № 9
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

**ПЕРЕЧЕНЬ**
**ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ**
**ИНСТИТУТА**

| № п/п | Наименование | Класс |
|---|---|---|
| 1. | "1С-Бухгалтерия" | К2 специальная |
| 2. | "Парус" | К2 специальная |
| 3. | УРМ "Криста" | К3 специальная |
| 4. | "АИС по плану проспекту курсовых мероприятий" | К2 специальная |
| 5. | СДО "Moodle" http://kpk.staviropk.ru/ | К2 специальная |
| 6. | СДО "Moodle" http://dodi.stavcdo.ru/ | К2 специальная |
| 7. | Сайт "Государственное бюджетное учреждение дополнительного профессионального образования «Ставропольский краевой институт развития образования, повышения квалификации и переподготовки работников образования»" http://cdo.staviropk.ru/ | К2 специальная |
| 8. | Сайт "Дистанционное обучение детей-инвалидов в Ставропольском крае" http://www.stavcdo.ru/ | К2 специальная |
| 9. | "ABBYY TestReader " | К2 специальная |

Приложение № 10
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

**ПЕРЕЧЕНЬ**
**ДОЛЖНОСТЕЙ РАБОТНИКОВ ИНСТИТУТА, ЗАМЕЩЕНИЕ КОТОРЫХ ПРЕДУСМАТРИВАЕТ ОСУЩЕСТВЛЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЛИБО ОСУЩЕСТВЛЕНИЕ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ**

| № п/п | Наименование структурного подразделения | Наименование должности |
|---|---|---|
| 1. | Ректорат | Ректор |
| | | Проректор по учебно-организационной работе |
| | | Проректор по научно-инновационной работе |
| | | Проректор по информатизации и региональному развитию системы образования |
| 2. | Планово-финансовый отдел | Главный бухгалтер |
| | | Заместитель главного бухгалтера |
| | | Ведущий бухгалтер |
| | | Главный экономист |
| | | Экономист по МТС |
| 3. | Отдел кадрового и правового обеспечения | Начальник отдела |
| | | Ведущий юрисконсульт |
| | | Юрисконсульт |
| | | Специалист по кадрам |
| | | Секретарь руководителя |
| | | Архивариус |
| 4. | Отдел планирования и организации учебной деятельности | Начальник отдела |
| | | Специалист по учебно-методической работе |

| | | |
|---|---|---|
| 5. | Отдел аттестации педагогических работников | Начальник отдела |
| | | Методист |
| | | Специалист по учебно-методической работе |
| | | Старший лаборант |
| 6. | Отдел материально-технического обеспечения | Начальник отдела |
| | | Инженер |
| | | Специалист по охране труда |
| 7. | Общежитие | Заведующий общежитием |
| 8. | Организационно-методический отдел | Начальник отдела |
| | | Заместитель начальника |
| | | Методист |
| 9. | Библиотека | Заведующий библиотекой |
| 10. | Центр дистанционного обучения и информационных технологий | Руководитель центра |
| | | Методист |
| | | Инженер |
| 11. | Кафедры | Профессор |
| | | Доцент |
| | | Старший преподаватель |
| | | Преподаватель |
| | | Специалист по учебно-методической работе |
| 12. | Региональный центр обработки информации | Руководитель центра |
| | | Начальника отдела |
| | | Аналитик |
| | | Инженер |
| | | Программист |
| | | Техник |

Приложение № 11
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

**ПЕРЕЧЕНЬ**
**ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, РАЗРЕШЕННОГО К ИСПОЛЬЗОВАНИЮ В ИНСТИТУТЕ**

1. Операционные системы: семейства "Microsoft Windows"; семейства "Linux".

2. Средства Microsoft Office; LibreOffice. OpenOffice

3. Программное обеспечение бухгалтерского учета:

1С Предприятие 8.Х, "Парус ";"Удаленное место бюджетополучателя"; АС "Клиент-Сбербанк"; "Налогоплательщик ЮЛ"; "НД СПУ"; "Криста" "УРМ АС Бюджет";"Барс Балансодержатель"

4. Антивирусное программное обеспечение: "Dr.Web", "Nod 32"; "Kaspersky Antivirus".

5. Средства криптографической защиты информации:

"Крипто-ПроCSP"; "Rutoken Drivers", "VipNet Client", "Dallas Lock"

6. Программное обеспечение для просмотра электронной почты:

"The Bat!"; "Mozilla Thunderbird".

7. Интернет браузеры: "internet Explorer"; "Mozilla Firefox"; "Opera","Google.Chrome", "Яндекс браузер".

8. Программное обеспечение для архивирования файлов и папок (архиваторы): "WinRar"; "7Zip".

9. Программное обеспечение ABBYY Fine Reader, ABBYY TestReader..

10. Программное обеспечение Adobe Flash Player.

11. Программное обеспечение Adobe Acrobat Reader; Windows Djview.

12. Справочно-правовая система: "Консультант Плюс".

13. Программный комплекс "Nero".

14. Специализированное программное обеспечение, необходимое для обработки массивов данных, для достижения целей поставленных руководством института.

Приложение № 12
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

# ПЕРЕЧНИ
# ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНСТИТУТЕ

1. Перечень персональных данных, обрабатываемых в институте:

1) фамилия, имя, отчество;

2) дата рождения;

3) пол;

4) место рождения;

5) информация о смене фамилии;

6) гражданство;

7) адрес регистрации по месту жительства;

8) адрес фактического проживания;

9) данные документ, удостоверяющего личность субъекта персональных данных;

10) номер телефона, факса, адрес электронной почты;

11) индивидуальный налоговый номер;

12) номер страхового свидетельства обязательного пенсионного страхования;

13) данные на доверенное лицо;

14) сведения о социальных льготах и о социальном статусе;

15) номер страхового медицинского полиса обязательного медицинского страхования граждан;

16) информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающих образование (наименование, номер, дата выдачи, специальность, квалификация);

17) информация о трудовой деятельности до приема на работу;

18) информация о трудовом стаже (место работы, должность, период работы, причины увольнения);

19) информация о знании иностранных языков;

20) ученая степень, ученое звание;

21) денежное содержание, оклад:

22) справка с Главного управления министерства внутренних дел Российской Федерации по Ставропольскому краю об отсутствии судимости;

23) данные об эффективном контракте (номер, дата заключения, вид работы, наличие испытания, режим труда, длительность основанного и дополнительных отпусков, дополнительные социальные льготы и гарантии, характер работы, форма оплаты, условия труда, продолжительность рабочей недели, система оплаты);

24) сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);

25) данные об аттестации;

26) данные о повышении квалификации;

27) информация о профессиональной переподготовке, стажировке;

28) данные о наградах, поощрениях, почетных званиях;

29) информация о дисциплинарных взысканиях, судимостях, исполнительных листах;

30) информация о приеме на работу, перемещении по должности, увольнении;

31) информация об отпусках;

32) информация о командировках;

33) медицинское заключение о состоянии здоровья;

34) информация о государственном/негосударственном пенсионном обеспечении;

35) реквизиты банковского счета;

36) данные о семейном положении, составе семьи, сведения о близких родственниках;

37) сведения о доходах, об имуществе и обязательствах имущественного характера, о доходах, об имуществе и обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей;

38) фотография.

Приложение № 13
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

# ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНСТИТУТЕ

1. Ответственный за обработку персональных данных в своей работе руководствуется законодательством Российской Федерации в области персональных данных.

2. Ответственный за обработку персональных данных:

1) организовывает принятие правовых, организационных и технических мер для обеспечения защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

2) осуществляет контроль за соблюдением требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

3. Ответственный за обработку персональных данных вправе иметь доступ к информации, касающейся обработки персональных данных в институте и включающей:

а) цели обработки персональных данных;

б) категории обрабатываемых персональных данных;

в) категории субъектов, персональные данные которых обрабатываются;

г) правовые основания обработки персональных данных;

д) перечень действий с персональными данными, общее описание используемых в институте способов обработки персональных данных;

е) описание мер, предусмотренных статьями 18.1 и 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

ж) дату начала обработки персональных данных;

з) срок или условия прекращения обработки персональных данных;

и) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

к) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;

4. Ответственный за обработку персональных данных несет ответственность, предусмотренную законодательством Российской Федерации, за неисполнение (не надлежащее исполнение) возложенных обязанностей по организации обработки персональных данных в институте.

Приложение № 14
к приказу СКИРО ПК и ПРО
от «12» мая 2017 г. № 143/1-о/д

# ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ АДМИНИСТРАТОРА СЕТИ

1. Администратор сети в своей работе руководствуется нормативными правовыми актами, другими методическими материалами и нормативными документами, касающимися методов программирования и использования вычислительной техники при обработке информации и применения современных информационных технологий.

2. В функциональные обязанности администратора входит:

Поддерживает бесперебойное функционирование локальной компьютерной сети.

Осуществляет поддержку функционирования баз данных компьютерной сети.

Обеспечивает целостность данных, защиту их от несанкционированного доступа, регулирует права доступа пользователей сети к ресурсам компьютерной сети.

Выполняет установленные требования по резервному копированию данных компьютерной сети.

Использует стандартные и специальные средства регистрации и учета доступа к информации компьютерной сети.

Применяет оптимальные методы программирования с целью наиболее полного использования средств и возможностей компьютерной техники.

Ведет журналы, необходимые для нормального функционирования компьютерной сети.

Проводит обучение пользователей компьютерной сети.

Определяет возможность использования готовых программ, выпущенных другими организациями, осуществляет их внедрение.

Участвует в разработке исходных данных и постановке задач на модернизацию компьютерной сети.

Рассматривает на стадии согласования проектную документацию по совершенствованию систем контроля доступа на соответствие требованиям руководящих документов и техническому заданию, при необходимости вносит соответствующие корректировки.

Обеспечивает информационную безопасность компьютерной сети.

Разрабатывает правила эксплуатации компьютерной сети, определяет полномочия пользователей компьютерной сети по доступу к ресурсам компьютерной сети, осуществляет административную поддержку (настройку, контроль и оперативное реагирование на поступающие сигналы о нарушениях

установленных правил доступа, анализ журналов регистрации событий безопасности и т.п.).

Участвует в разработке технологии обеспечения информационной безопасности института, предусматривающей порядок взаимодействия подразделений института по вопросам обеспечения безопасности при эксплуатации компьютерной сети и модернизации ее программных и аппаратных средств.

Предотвращает несанкционированные модификации программного обеспечения, добавления новых функций, несанкционированный доступ к информации, аппаратуре и другим общим ресурсам компьютерной сети.

Осуществляет сопровождение и, при необходимости, доработку внедренных программных средств по информационной защите.

Разрабатывает способы и методы организации доступа пользователей компьютерной сети к ресурсам компьютерной сети.

Информирует работников института об уязвимых местах компьютерной сети, возможных путях несанкционированного доступа и воздействия на компьютерную сеть, известных компьютерных вирусах.

Ведет журнал системной информации, иную техническую документацию.

3. Администратор сети несет ответственность, предусмотренную законодательством Российской Федерации, за неисполнение (не надлежащее исполнение) возложенных обязанностей.