

**муниципальное автономное учреждение
дополнительного профессионального образования
«Новосибирский Институт Современного Образования»
(МАУ ДПО «НИСО»)**



УТВЕРЖДАЮ
Директор МАУ ДПО «НИСО»

/ М.Е. Давыдов
приказ № 85 от «01» 09 2022 г.

**ПОЛОЖЕНИЕ
о защите, хранении, обработке и передаче персональных данных
работников МАУ ДПО «НИСО»**

1. Общие Положения

1.1. Настоящее Положение о защите, хранении, обработке и передаче персональных данных работников муниципального автономного учреждения дополнительного профессионального образования «Новосибирский Институт Современного Образования» (далее – Положение) разработано в целях предотвращения несанкционированного доступа к персональным данным работников, неправомерного использования или их утраты.

1.2. Положение устанавливает процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

1.3. Положение разработано в соответствии с:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации (далее - ТК РФ);
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - ФЗ № 152);
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ № 149);
- иными нормативными правовыми актами в области обработки и защиты персональных данных.

Все вопросы, связанные с обработкой персональных данных, не урегулированные настоящим Положением, разрешаются в соответствии с действующим законодательством Российской Федерации в области персональных данных.

1.4. Муниципальное автономное учреждение дополнительного профессионального образования «Новосибирский Институт Современного Образования» (далее – Институт) в соответствии с ФЗ № 152 является оператором, осуществляющим обработку персональных данных, а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (далее – оператор персональных данных).

2. Основные понятия

2.1. Основные понятия:

- **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

- **персональные данные, разрешенные субъектом персональных данных для распространения** - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном ФЗ № 152;

- **Оператор** - учреждение, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

- **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

- **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

- **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации

определить принадлежность персональных данных конкретному субъекту персональных данных;

- **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.2. К персональным данным работников, получаемых Институтом и подлежащим хранению в порядке, предусмотренном действующим законодательством РФ и настоящим Положением, относятся следующие сведения, содержащиеся в личных делах работников:

- фамилия, имя, отчество;
- дата и место рождения;
- паспортные данные;
- адрес места жительства;
- номер телефона;
- адрес электронной почты;
- сведения о гражданстве;
- сведения о занимаемой ранее должности и стаже работы;
- сведения об образовании (реквизитах документов об образовании, квалификации и наличии специальных знаний), сведения о профессиональной переподготовке и (или) повышении квалификации (реквизитах документов);
- сведения об идентификационном номере налогоплательщика (ИНН);
- сведения о номере и серии страхового свидетельства государственного пенсионного страхования (СНИЛС);
- сведения о наличии или отсутствии судимости;
- сведения о воинской обязанности, воинском учете;
- сведения о состоянии здоровья (реквизиты полиса обязательного медицинского страхования, иных документов, содержащих сведения о состоянии здоровья);
- сведения о семейном положении и составе семьи работников;
- сведения о льготах;
- сведения об имущественном положении, доходах, задолженности;
- сведения об использованных отпусках;
- сведения об имеющихся наградах (поощрениях), почётных званиях;
- фотографии;
- видеозаписи;
- иные сведения, необходимые Институту в соответствии с действующим законодательством РФ в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных.

2.3. Персональные данные работников Института являются конфиденциальной информацией и не могут быть использованы Институтом или любым другим лицом в личных целях.

2.4. Институт и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия работников, если иное не предусмотрено законодательством РФ.

3. Обработка, хранение и передача персональных данных работника

3.1. Обработка персональных данных должна осуществляться на законной и справедливой основе и ограничиваться достижением конкретных, заранее определенных и законных целей.

3.2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

3.3. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. **(Приложение № 1 к настоящему положению).**

3.4. Лицо, осуществляющее обработку персональных данных по приказу директора Института, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные ФЗ № 152, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных ФЗ № 152.

3.5. Обработка персональных данных в информационных системах Института (далее - информационные системы персональных данных) осуществляется в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.6. Обеспечение безопасности персональных данных в информационных системах персональных данных достигается путем:

а) определения угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

б) применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

в) применения прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

г) оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем персональных данных;

д) учета машинных носителей персональных данных;

е) обнаружения фактов несанкционированного доступа к персональным данным и принятием мер по прекращению несанкционированного доступа;

ж) восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

з) установления правил доступа (пароль, логин и др.) к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных.

3.7. Институт обрабатывает в информационных системах с использованием средств автоматизации и обеспечивает защиту с учетом определенного типа угроз

безопасности и уровня защищенности персональных данных следующие категории персональных данных работников:

Категория персональных данных	Перечень персональных данных	Категория субъектов персональных данных	Тип угрозы/уровень защищенности	Срок обработки/срок хранения
1. Общие персональные данные	<ul style="list-style-type: none"> - фамилия, имя, отчество; - гражданство; - год, месяц, дата рождения; - место рождения; - адрес; - сведения об образовании; - номер телефона; - СНИЛС; - ИНН; - сведения о воинском учёте; - иное. 	Работники	3 тип угрозы/4 уровень защищенности	до прекращения трудовых отношений
2. Общие и специальные персональные данные	<ul style="list-style-type: none"> - фамилия, имя, отчество; - гражданство; - год, месяц, дата рождения; - место рождения; - адрес; - сведения об образовании; - номер телефона; - СНИЛС; - ИНН; - сведения о воинском учёте; - расовая, национальная принадлежности; - состояние здоровья; - иное. 	Работники	3 тип угрозы/ 3 уровень защищенности	до прекращения трудовых отношений
3. Общие и биометрические персональные данные	<ul style="list-style-type: none"> - фамилия, имя, отчество; - гражданство; - год, месяц, дата рождения; - место рождения; - адрес; 	Работники	3 тип угрозы/3 уровень защищенности	до прекращения трудовых отношений

	<ul style="list-style-type: none"> - сведения об образовании; - номер телефона; - СНИЛС; - ИНН; - сведения о воинском учёте; - фото; - видео; - иное. 			
--	---	--	--	--

3.8. При 4-м уровне защищенности персональных данных Институт:

- обеспечивает режим безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечивает сохранность носителей персональных данных;

- утверждает перечень работников, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими трудовых обязанностей;

- использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

3.9. При 3-м уровне защищенности персональных данных Институт дополнительно к мерам, перечисленным в п. 3.8 настоящего Положения, назначает должностное лицо (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

3.10. Институт обрабатывает без использования средств автоматизации и обеспечивает защиту следующие категории персональных данных работника, которые хранятся на бумажных носителях:

Категория персональных данных	Перечень персональных данных	Категория субъектов персональных данных	Срок обработки/срок хранения
1. Общие персональные данные	<ul style="list-style-type: none"> - фамилия, имя, отчество; - гражданство; - год, месяц, дата рождения; - место рождения; - адрес; - сведения об образовании; - номер телефона; - СНИЛС; - ИНН; - сведения о воинском учёте; - иное. 	Работники	до прекращения трудовых отношений

2. Общие и специальные персональные данные	<ul style="list-style-type: none"> - фамилия, имя, отчество; - гражданство; - год, месяц, дата рождения; - место рождения; - адрес; - сведения об образовании; - номер телефона; - СНИЛС; - ИНН; - сведения о воинском учёте; - расовая, национальная принадлежности; - состояние здоровья, - иное. 	Работники	до прекращения трудовых отношений
3. Общие и биометрические персональные данные	<ul style="list-style-type: none"> - фамилия, имя, отчество; - гражданство; - год, месяц, дата рождения; - место рождения; - адрес; - сведения об образовании; - номер телефона; - СНИЛС; - ИНН; - сведения о воинском учёте; - фото; - иное. 	Работники	до прекращения трудовых отношений

3.11. Институт при обработке персональных данных работника на бумажных носителях в целях обеспечения их защиты:

- назначает должностное лицо (работника), ответственного за обработку персональных данных;

- ограничивает допуск в помещения, в которых хранятся документы, содержащие персональные данные работников.

3.12. В целях обеспечения конфиденциальности документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только специалистом по кадрам.

3.13. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством РФ, допускается исключительно с согласия субъекта персональных данных на обработку его

персональных данных в части их предоставления или согласия на распространение персональных данных.

3.14. Передача информации, содержащей сведения о персональных данных работников по телефону, в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

3.15. Персональные данные работников на бумажном носителе хранятся в личном деле в специально отведенном помещении Института, предназначенном для обработки персональных данных без использования средств автоматизации (**Приложение № 2 к настоящему положению**).

3.16. Помещения, в которых располагаются технические средства информационных систем персональных данных или хранятся носители персональных данных, должны соответствовать требованиям пожарной безопасности, установленным действующим законодательством РФ.

3.17. Молчание или бездействие работника ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных им для распространения.

4. Доступ к персональным данным работника

4.1. Право доступа к персональным данным работника имеют:

- директор;
- заместитель директора;
- заместитель директора - руководитель структурного подразделения;
- главный бухгалтер;
- специалист по кадрам;
- бухгалтер;
- контрактный управляющий;
- начальник отдела технической поддержки;
- начальник отдела оценочных процедур;
- начальник отдела мониторинга и повышения качества образования;
- начальник отдела цифровизации образования;
- начальник отдела медиа-сопровождения;
- начальник отдела фото-видео-сопровождения;
- специалист по административно-хозяйственной деятельности;
- главный инженер;
- начальник отдела юридической поддержки;
- начальник отдела организационной работы;
- начальник отдела профессионального роста педагогов и руководителей;
- начальник отдела развития дополнительного образования детей;
- начальник отдела методического сопровождения воспитания детей;
- начальник отдела выявления, развития, поддержки способностей и талантов детей;
- работник.

4.2. Институт вправе осуществлять передачу персональных данных работника третьим лицам, в том числе в коммерческих целях, только с его предварительного письменного согласия, за исключением случаев, когда это необходимо в целях

предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных действующим законодательством Российской Федерации.

Перед передачей персональных данных Институт должен предупредить третье лицо о том, что они могут быть использованы только в тех целях, для которых были сообщены. При этом у третьего лица необходимо получить подтверждение того, что такое требование будет им соблюдено.

Не требуется согласие работника на передачу персональных данных:

- третьим лицам в целях предупреждения угрозы жизни и здоровью работника;
- в Фонд социального страхования Российской Федерации, Пенсионный фонд Российской Федерации в объеме, предусмотренном действующим законодательством Российской Федерации;
- в налоговые органы;
- в военные комиссариаты;
- по запросу профессиональных союзов в целях контроля за соблюдением трудового законодательства работодателем;
- по мотивированному запросу органов прокуратуры;
- по мотивированному требованию правоохранительных органов и органов безопасности;
- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности;
- по запросу суда;
- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом;
- в случаях, связанных с исполнением работником должностных обязанностей;
- в кредитную организацию, обслуживающую платежные карты работников.

4.3. Сведения о работнике (в том числе уволенном) могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника.

4.4. Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника.

5. Обязанности Института по хранению и защите персональных данных

5.1. Институт за свой счет обеспечивает защиту персональных данных работников от неправомерного их использования или утраты в порядке, установленном законодательством РФ.

5.2. Институт самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных ФЗ № 152 и принятыми в соответствии с ним нормативными правовыми актами.

К таким мерам, в частности, относятся:

- 1) назначение ответственного за организацию обработки персональных данных;
- 2) издание документов, определяющих политику Института в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их

обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на Институт, не предусмотренные законодательством Российской Федерации полномочия и обязанности;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных ФЗ № 152 и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Института в отношении обработки персональных данных, его локальным нормативным актам;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ № 152, соотношение указанного вреда и принимаемых Институтом мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ № 152;

6) ознакомление работников Института, непосредственно осуществляющих обработку персональных данных, с требованиями ФЗ № 152, в том числе требованиями к защите персональных данных, документами, определяющими политику Института в отношении обработки персональных данных, локальными нормативными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

5.3. Институт знакомит работников с настоящим Положением и их правами в области защиты персональных данных.

5.4. Институт осуществляет передачу персональных данных работников только в соответствии с настоящим Положением и законодательством РФ.

5.5. Институт предоставляет персональные данные работника только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей, в соответствии с настоящим положением и законодательством РФ.

5.6. Институт обеспечивает работникам свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных законодательством РФ.

5.7. Институт по требованию работника предоставляет ему полную информацию о его персональных данных и обработке этих данных.

5.8. Работники Института, имеющие доступ к информационным системам персональных данных, обязаны:

- принимать меры, исключая несанкционированный доступ к используемым программно-техническим средствам;

- вести учет электронных носителей информации, содержащих персональные данные, и осуществлять их хранение в металлических шкафах или сейфах;
- производить запись персональных данных (отдельных файлов, баз данных) на электронные носители только в случаях, регламентированных порядком работы с персональными данными;
- соблюдать установленный порядок и правила доступа в информационные системы, не допускать передачу персональных кодов и паролей к информационным системам персональных данных;
- принимать все необходимые меры к надежной сохранности кодов и паролей доступа к информационным системам персональных данных;
- работать с информационными системами персональных данных в объеме своих полномочий, не допускать их превышения;
- обладать навыками работы с антивирусными программами в объеме, необходимом для выполнения функциональных обязанностей и требований по защите информации.

5.9. При работе работников Института в информационных системах персональных данных запрещается:

- записывать значения кодов и паролей доступа к информационным системам персональных данных;
- передавать коды и пароли доступа к информационным системам персональных данных другим лицам;
- пользоваться в работе кодами и паролями других пользователей доступа к информационным системам персональных данных;
- производить подбор кодов и паролей доступа к информационным системам персональных данных других пользователей;
- записывать на электронные носители с персональными данными посторонние программы и данные;
- копировать информацию с персональными данными на неучтенные электронные носители информации;
- выносить электронные носители с персональными данными за пределы территории Института;
- покидать рабочее место с включенным персональным компьютером без применения аппаратных или программных средств блокирования доступа к персональному компьютеру;
- приносить, самостоятельно устанавливать и эксплуатировать на персональном компьютере любые программные продукты, не принятые к эксплуатации;
- открывать, разбирать, ремонтировать персональные компьютеры, вносить изменения в конструкцию, подключать нештатные блоки и устройства;
- передавать информацию, содержащую персональные данные, подлежащие защите, по открытым каналам связи (факсимильная связь, электронная почта и иное), а также использовать сведения, содержащие персональные данные, подлежащие защите, в открытой переписке и при ведении переговоров по телефону.

5.10. При смене работника, ответственного за учет документов на бумажном носителе, содержащих персональные данные, составляется акт приема-сдачи этих материалов, который утверждается приказом директора Института.

5.11. При работе с документами, содержащими персональные данные на бумажном носителе, уполномоченные на обработку персональных данных работники Института обязаны:

- ознакомиться только с теми документами, содержащими персональные данные, к которым получен доступ в соответствии со служебной необходимостью;

- хранить в тайне ставшие известными им сведения, содержащие персональные данные, подлежащие защите, информировать непосредственного руководителя о фактах нарушения порядка работы с персональными данными и о попытках несанкционированного доступа к ним;

- о допущенных нарушениях установленного порядка работы, учета и хранения документов, содержащих персональные данные, а также о фактах разглашения сведений, содержащих персональные данные, подлежащих защите, представлять непосредственным руководителям письменные объяснения.

5.12. Ответственный за обработку персональных данных работников Института обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

5.13. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, ответственный за обработку персональных данных обязан с момента выявления такого инцидента ответственным, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

- 1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента;

- 2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

5.14. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в настоящем Положении, Институт осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5.15. После истечения срока нормативного хранения документов, содержащих персональные данные работника, или при наступлении иных законных оснований документы подлежат уничтожению.

5.16. Институт для этих целей создает экспертную комиссию и проводит экспертизу ценности документов.

5.17. По результатам экспертизы документы, содержащие персональные данные работника и подлежащие уничтожению:

- на бумажном носителе - уничтожаются путем измельчения или сжигания;
- в электронном виде - стираются с информационных носителей либо физически уничтожаются сами носители, на которых хранится информация.

6. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

6.1. Процедурами, направленными на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, являются:

- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных;

- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых Институтом мер, направленных на обеспечение выполнения обязанностей оператора персональных данных, предусмотренных Федеральным законом;

- ознакомление работников Института непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, с требованиями по защите персональных данных.

6.2. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором персональных данных, оператор персональных данных в срок, не превышающий 3 рабочих дня с даты выявления неправомерной обработки персональных данных, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор персональных данных в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении неправомерной обработки персональных данных или об уничтожении персональных данных оператор персональных данных обязан уведомить субъекта персональных данных или его представителя.

6.3. В случае достижения цели обработки персональных данных оператор персональных данных обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 рабочих дней с даты достижения цели обработки персональных данных.

6.4. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор персональных данных обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 дней с даты получения указанного отзыва. Об уничтожении персональных данных оператор персональных данных в течении трех рабочих дней обязан уведомить субъекта персональных данных.

6.5. В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор обязан в срок,

не превышающий десяти рабочих дней с даты получения оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных, частью 2 статьи 10 и частью 2 статьи 11 ФЗ № 152. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными Федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

7.2. Моральный вред, причиненный Работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником убытков.

8. Заключительные положения

8.1. Настоящее Положение вступает в силу с момента утверждения приказом директора Института.

8.2. Изменения и (или) дополнения утверждаются приказом директора Института.

8.3. Настоящее Положение доводится до сведения всех работников персонально под подпись.

Приложение № 1
к Положению о защите, хранении, обработке и передаче
персональных данных работников МАУ ДПО «НИСО»

СОГЛАСИЕ
на обработку персональных данных
МАУ ДПО «НИСО»

Я, _____

(фамилия, имя отчество, год рождения)

зарегистрированный по адресу: _____

паспорт серия ____ номер _____, выдан _____

(дата выдачи, орган выдавший, код подразделения)

в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», в своей воле и в своем интересе даю согласие муниципальному автономному учреждению дополнительного профессионального образования «Новосибирский Институт Современного Образования», расположенному по адресу: г. Новосибирск, ул. Котовского, 8, на обработку персональных данных со следующими условиями:

1. Настоящее согласие дается на обработку персональных данных работником как без использования средств автоматизации, так и с их использованием.

2. Согласие дается на обработку следующих персональных данных:

1) общие персональные данные: фамилия, имя, отчество; дата и место рождения; паспортные данные; адрес места жительства; номер телефона; адрес электронной почты; сведения о гражданстве; сведения о занимаемой ранее должности и стаже работы; сведения об образовании (реквизитах документов об образовании, квалификации и наличии специальных знаний), сведения о профессиональной переподготовке и (или) повышении квалификации (реквизитах документов); сведения об идентификационном номере налогоплательщика (ИНН); сведения о номере и серии страхового свидетельства государственного пенсионного страхования (СНИЛС); сведения о воинской обязанности, воинском учете; сведения о льготах; сведения об имущественном положении, доходах, задолженности; сведения о расчетном счете и банковской карты (реквизиты указанных документов); иные сведения, необходимые Учреждению в соответствии с действующим законодательством РФ в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных;

2) специальные персональные данные: национальная принадлежность и раса, сведения о наличии или отсутствии судимости; сведения о состоянии здоровья (реквизиты полиса обязательного медицинского страхования, иных документов, содержащих сведения о состоянии здоровья); сведения о семейном положении и составе семьи работников;

3) биометрические данные: фотографии, видеозаписи, на которых возможно идентифицировать субъекта персональных данных.

3. Настоящее согласие дается для следующих целей: обеспечение соблюдения требований законодательства Российской Федерации; оформление и регулирование трудовых отношений; организации кадрового учета; обеспечения безопасности, ведения кадрового делопроизводства, начисления заработной платы, содействия работникам в трудоустройстве, обучении и продвижении по службе, пользования различного вида льготами; исполнения требований

налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также пенсионного законодательства при формировании и представлении персоналицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации, в соответствии с законодательством РФ.

4. Настоящее согласие предоставляется на осуществление любых действий в отношении персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, предоставление (по запросам правоохранительных органов, решению суда и в прочих случаях, предусмотренных законодательством РФ), блокирование, уничтожение, персональных данных, а также осуществление любых иных действий с моими персональными данными с учетом федерального законодательства.

5. Персональные данные могут передаваться третьим лицам для достижения указанных выше целей в соответствии в пределах, предусмотренных законодательством РФ.

6. В соответствии с положениями части 2 статьи 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» субъект персональных данных имеет право отозвать настоящее согласие. Согласие может быть отозвано субъектом персональных данных или его представителем путем направления письменного заявления в адрес наименование Учреждения.

7. В случае отзыва субъектом персональных данных или его представителем согласия на обработку персональных данных наименование учреждения вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в п. 2 — 11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

8. Подтверждаю, что ознакомлен(а) с положением о защите, хранении, обработке и передачи персональных данных работников МАУ ДПО «НИСО».

9. Мне разъяснены права и обязанности в области защиты персональных данных, а также право работодателя обрабатывать (в том числе и передавать) часть моих персональных данных без моего согласия, в соответствии с законодательством Российской Федерации.

10. Настоящее согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока трудовой деятельности.

/

« » 20 г.

Приложение № 2
к Положению о защите, хранении, обработке и передаче
персональных данных работников МАУ ДПО «НИСО»

Список помещений, предназначенных для обработки персональных данных без
использования средств автоматизации

№ п/п	Наименование помещения	Место хранения носителей персональных данных	Адрес расположения помещения
1	Кабинет специалиста по кадрам	Архив	630032, г. Новосибирск, ул. Котовского, д. 8