УТВЕРЖДАЮ
Ректор АОУ ВО ДПО «Вологодский институт развития образования»

_____ И.А. Макарьина
«23» апреля 2018 года

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных автономного образовательного учреждения Вологодской области дополнительного профессионального образования «Вологодский институт развития образования» по работе с персональными данными

1. Общие положения

1.1. Сотрудники автономного образовательного учреждения Вологодской области дополнительного профессионального образования «Вологодский институт развития образования» (далее – Учреждение), участвующие в обработке персональных данных (далее – ПДн) в информационных системах персональных данных (далее по тексту – Пользователи), осуществляют обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несёт персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется должностными инструкциями и организационно-распорядительными документами (далее – ОРД), в том числе утверждёнными в Учреждении в рамках обеспечения информационной безопасности ИСПДн.

1.5. Методическое руководство работой Пользователя осуществляется ответственным лицом за обработку ПДн (в соответствии с зонами ответственности) в Учреждении.

2. Обязанности Пользователя

2.1. Пользователь обязан соблюдать порядок обеспечения конфиденциальности при обращении с информацией, содержащей ПДн, ставшей ему известной (или доступной для обработки) в процессе работы. Свои обязательства по сохранению конфиденциальности при обращении с информацией, содержащей ПДн, он подтверждает при заключении трудового договора, подписывая «Обязательство о неразглашении персональных данных».

2.2. Пользователь обязан знать и выполнять требования действующих нормативных и руководящих документов в области защиты ПДн, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите сведений, отнесённых к категории «Персональные данные».

2.3. Пользователь должен выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые входят в его компетенцию.

2.4. Пользователь должен знать и соблюдать установленные требования по режиму обработки ПДн, учёту, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.5. Пользователь должен соблюдать требования парольной политики, представленной в «Инструкции по организации парольной защиты».

2.6. Экран монитора в помещении Пользователя, где обрабатываются ПДн, Пользователь должен располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нём информацией посторонними лицами.

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью ПДн, обрабатываемых в ИСПДн, а также для консультаций по вопросам обеспечения безопасности ПДн Пользователь должен обращаться к ответственному лицу за обработку персональных данных (в соответствии с зонами ответственности) (далее – Ответственный).

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн Пользователю необходимо обращаться к начальнику отдела информационно-коммуникационных технологий.

2.9. Пользователям запрещается:

- Разглашать защищаемую информацию третьим лицам.
- Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.
- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
- Несанкционированно открывать общий доступ к папкам на своем рабочем месте.
- Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.
- Отключать (блокировать) средства защиты информации.
- Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.
- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.
- Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

- Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий в пределах возложенных на него функций.
- Использовать на АРМ, входящих в состав ИСПДн и обрабатывающих ПДн, коммуникационные сервисы сторонних лиц (провайдеров) (ICQ, Skype и иных сервисов).
- Запрещается на АРМ, входящих в состав ИСПДн и обрабатывающих ПДн, использование технологий передачи видеоинформации.

3. Ответственность Пользователя

Пользователь несет персональную ответственность за невыполнение требований настоящей Инструкции.

3.1. Согласно статье 90 Трудового кодекса Российской Федерации, ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника: лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

3.2. Незаконный сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации и (или) совершенные лицом с использованием своего служебного положения подпадает под действие статьи 137 Уголовного кодекса Российской Федерации «Нарушение неприкосновенности частной жизни».

3.3. Отказ в предоставлении гражданину информации. Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан подпадает под действие статьи 140.

3.4. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации подпадает под действие статьи 272 Уголовного кодекса Российской Федерации «Неправомерный доступ к компьютерной информации».