	Министерство образования и молодежной политики Свердловской области
	Государственное автономное профессиональное образовательное учреждение Свердловской области «Екатеринбургский техникум химического машиностроения»
	Инструкция по правилам обработки ПД

Рассмотрено
на заседании Совета
ГАПОУ СО «ЕТХМ»
Протокол № 3,
от « 31 » января 2020 г.

УТВЕРЖДЕНО
Приказом директора
ГАПОУ СО «ЕТХМ»
№ 24 - о/д от « 03 » февраля 2020 г.

ИНСТРУКЦИЯ
ПО ПРАВИЛАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСУДАРСТВЕННОМ АВТОНОМНОМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ СВЕРДЛОВСКОЙ ОБЛАСТИ «ЕКАТЕРИНБУРГСКИЙ ТЕХНИКУМ ХИМИЧЕСКОГО МАШИНОСТРОЕНИЯ»

Екатеринбург
2020 г.

Введено в действие с 03.02.2020 г.

1. Общие положения

1.1. Настоящая Инструкция разработана на основании:

- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

1.2. Настоящая Инструкция устанавливает правила работы с документами, содержащими персональные данные.

1.3. Настоящая Инструкция разработана в целях:

- предотвращения неконтролируемого распространения конфиденциальной информации, содержащей персональные;
- предотвращения несанкционированного уничтожения, искажения, копирования, блокирования информации, содержащей персональные данные;
- предотвращения утраты, несанкционированного уничтожения или сбоев в процессе функционирования автоматизированных систем обработки информации, содержащей персональные данные;
- соблюдения правового режима использования информации, содержащей персональные данные.

1.4. К персональным данным относятся:

- анкетные и биографические данные гражданина, включая адрес места жительства;
- паспортные данные или данные иного документа, удостоверяющего личность и гражданство, включая серию, номер, дату выдачи, наименование органа, выдавшего документ);
- сведения об образовании, квалификации, наличии специальных знаний или специальной подготовки;
- сведения о трудовой деятельности, опыте работы, занимаемой должности, трудовом стаже, повышении квалификации и переподготовки;
- сведения о составе семьи, а также сведения о месте работы или учёбы членов семьи;
- сведения о состоянии здоровья и наличии заболеваний;
- сведения об отношении к воинской обязанности;
- сведения о доходах и обязательствах имущественного характера, в том числе членов семьи;
- сведения об идентификационном номере налогоплательщика;
- реквизиты расчетных счетов в банках;

- сведения о социальных льготах и о социальном статусе гражданина и членов его семьи;
- сведения о решениях судебных органов, органов опеки в отношении гражданина и членов его семьи.

1.5. Сотрудники образовательной организации, в силу своих функциональных обязанностей участвующие в процессах обработки персональных данных (далее – пользователи), допускаются к работе с персональными данными на основании распоряжения руководителя образовательной организации и в соответствии с утвержденным списком лиц, допущенных к работе с персональными данными.

1.6. Методическое руководство работой пользователя осуществляется ответственными за эксплуатацию информационной системы/ответственными за организацию обработки персональных данных.

1.7. Согласие субъекта на обработку его персональных данных не требуется, если:

- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, а получение согласия субъекта невозможно;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных проводится по требованию уполномоченных на то государственных органов в случаях, предусмотренных федеральным законом;
- обработка персональных данных осуществляется в целях исполнения обращения, запроса самого субъекта персональных данных, трудового или иного договора с ним.

1.8. Субъект персональных данных имеет право требовать от оператора уточнения его персональных данных, их блокирования или уничтожения, в случае если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

1.9. Режим конфиденциальности персональных данных отменяется:

- в случае обезличивания персональных данных;
- в отношении персональных данных, ставших общедоступными;
- по истечении 75-летнего срока хранения персональных данных, если иное не предусмотрено законом.

1.10. Перед началом работы пользователь обязан изучить настоящую Инструкцию и ознакомиться с ответственностью за выполнение требований

Инструкции пользователя при работе с конфиденциальной информацией под роспись.

1.11. В своей деятельности пользователь руководствуется настоящей Инструкцией и действующим законодательством в сфере защиты персональных данных.

1.12. Пользователь несёт персональную ответственность за выполнение настоящей Инструкции в установленном законом порядке.

2. Организация работы

2.1. Пользователь должен иметь специальное рабочее место, размещённое на территории образовательной организации таким образом, чтобы исключить несанкционированный доступ к нему посторонних лиц и других сотрудников.

2.2. Автоматизированное рабочее место пользователя (далее – АРМ) размещается таким образом, чтобы исключить визуальный просмотр экрана видеомонитора лицами, не имеющими отношения к обрабатываемой информации.

2.3. АРМ должны быть защищены индивидуальными паролями доступа и средствами антивирусной защиты в соответствии с установленным порядком.

2.4. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним в соответствии с Инструкцией по организации хранения, учета и работы с материальными носителями, содержащими конфиденциальную информацию и персональные данные.

2.5. Не допускается без согласования с руководителем образовательной организации формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих персональные данные.

2.6. Пользователь взаимодействует с ответственными за эксплуатацию информационной системы/ответственными за организацию обработки персональных данных по вопросам обеспечения защиты персональных данных и подчиняется их распоряжениям.

3. Правила обработки персональных данных

3.1. Для каждой категории персональных данных должен использоваться отдельный материальный носитель.

3.2. В обязательном порядке обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.3. Не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы.

3.4. После подготовки и передачи документа файлы, копии, черновики документа переносятся подготовившим их должностным лицом на

маркированные носители, предназначенные для хранения персональных данных.

3.5. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна вестись таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей).

3.6. При использовании типовых форм документов, характер информации которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, 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 способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

3.7. При работе с материальными носителями, содержащими персональные данные, пользователь обязан исключить возможность ознакомления, просмотра этих документов лицами, не имеющими соответствующего допуска.

3.8. При работе с тетрадями/журналами, содержащими персональные данные обучающихся (в том числе – информацию о результатах освоения образовательной программы) не допускается:

- хранение указанных тетрадей/журналов вместе с носителями открытой информации;
- передача на хранение другим лицам;
- вынос тетрадей/журналов за пределы образовательной организации.

3.9. Передача персональных данных допускается только в случаях, установленных законодательством Российской Федерации и действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению уполномоченных лиц.

3.10. Передача персональных данных не допускается с использованием средств телекоммуникационных каналов связи без письменного согласия субъекта персональных данных, за исключением случаев, установленных законодательством Российской Федерации.

3.11. При выносе материальных носителей, содержащих персональные данные (в том числе распечаток текстов, графической и иной информации), за пределы служебного помещения, а так же при передаче материальных носителей и/или их копий пользователь обязан сделать отметку в соответствующем журнале/реестре учета материальных носителей.

3.12. 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.

3.13. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, но с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.14. Под обезличиванием персональных данных (далее – обезличивание) понимаются действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту.

3.15. Обезличивание может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

3.16. Решение о необходимости обезличивания принимает руководитель образовательной организации.

3.17. Способ обезличивания определяется руководителем образовательной организации/ответственным лицом.

3.18. К способам обезличивания персональных данных при условии их дальнейшей обработки, относятся:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение (понижение) точности некоторых сведений;
- деление сведений на части и обработка их в разных информационных системах.

3.19. Уничтожение обработанных персональных данных производится по решению специальной комиссии, сформированной приказом руководителя образовательной организации, с составлением соответствующего акта.

3.20. При утрате (утере, хищении) материальных носителей, содержащих персональные данные, пользователь обязан немедленно сообщить руководителю образовательной организации/ответственному лицу.

3.21. По факту утраты (утери, хищения) материальных носителей, содержащих персональные данные, назначается служебное расследование.

4. Обязанности пользователя

Пользователь обязан:

4.1. Выполнять только те процедуры обработки персональных данных, которые определены его обязанностями.

4.2. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных.

4.3. Обеспечить правильность ввода и коррекции персональных данных.

4.4. При работе со съемными носителями каждый раз перед началом работы проверить их на наличие вирусов с использованием штатных антивирусных программ. Соблюдать требования антивирусной защиты.

4.5. Осуществлять копирование необходимой информации по мере ее обновления на учтенные в установленном порядке носители.

4.6. Осуществлять использование, хранение, учет и утилизацию носителей персональных данных (бумажных и электронных) в соответствии с правилами, принятыми в образовательной организации.

4.7. Немедленно сообщать непосредственному руководителю/ ответственному лицу об утрате или недостаче носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению персональных данных.

4.8. Немедленно ставить в известность руководителя образовательной организации/ответственное лицо при:

- подозрении о компрометации личных идентификаторов и паролей;
- обнаружении нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа;
- обнаружении несанкционированных изменений в конфигурации программных или аппаратных средств АРМ;
- обнаружении некорректного функционирования установленных на АРМ технических средств защиты, непредусмотренных отводов кабелей и подключенных устройств;
- выходе из строя или неустойчивом функционировании узлов АРМ или периферийных устройств, а также перебоях в системе электроснабжения.

4.9. Соблюдать требования парольной политики и правила использования сети Интернет, принятые в образовательной организации.

4.10. При завершении сеанса работы/наступления перерыва в работе обеспечить невозможность доступа к персональным данным на время отсутствия пользователя на рабочем месте.

Пользователю запрещается:

4.11. Оставлять бесконтрольно включенное АРМ, материальные носители, содержащие персональные данные.

4.12. Сохранять обрабатываемую информацию на носителях, не предназначенных для хранения персональных данных.

4.13. Копировать информацию, содержащую персональные данные, на внешние носители без разрешения руководителя образовательной организации/администратора информационной системы.

4.14. Удалять или искажать программы и файлы, содержащие персональные данные.

4.15. Самовольно изменять состав и конфигурацию используемых программно-аппаратных средств, в т.ч. устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы.

4.16. Самовольно изменять настройки АРМ и информационной сети.

4.17. Самовольно изменять параметры средств защиты информации (в том числе средств парольной и антивирусной защиты).

4.18. Подключать к информационной системе личные средства вычислительной техники: ноутбуки, карманные компьютеры, смартфоны и т.п., а также личные носители и накопители информации без санкции руководителя образовательной организации/администратора информационной системы.

4.19. В случае возникновения неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

4.20. Разглашать информацию, содержащую персональные данные, третьим лицам.

4.21. Вести разговоры с третьими лицами о процедурах доступа к АРМ и информации, сообщать устно или письменно персональный пароль.

4.22. Разрешать посторонним лицам работать под своей учетной записью.

4.23. Привлекать третьих лиц для производства ремонта или настройки АРМ без согласования с руководителем образовательной организации и ответственными лицами.

4.24. Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

5. Права

Пользователь имеет право:

5.1. Осуществлять доступ к программным и аппаратным средствам информационной системы в пределах предоставленных полномочий и в соответствии с закрепленными за ним обязанностями.

5.2. Обращаться к техническим специалистам и руководству за необходимой технической и методической помощью.

5.3. Участвовать в анализе ситуаций, касающихся функционирования закрепленного за ним АРМ и рабочих программ.

5.4. Знакомиться с проектами решений руководства образовательной организации, касающимися его деятельности.

5.5. Вносить на рассмотрение руководства предложения по совершенствованию работы информационной системы и закрепленного за ним АРМ.

6. Ответственность

Пользователи несут ответственность за:

6.1. Неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации.

6.2. Причинение материального ущерба работодателю – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

6.3. Правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным, гражданским законодательством Российской Федерации.

С инструкцией ознакомлен:

ФИО	должность	подпись	дата