УТВЕРЖДАЮ
Директор Центра

А. В. Жигайлов
«31» марта 2021 г.

П О Р У Ч Е Н И Е
на обработку персональных данных субъектов государственного автономного образовательного учреждения дополнительного образования «Центр для одаренных детей «Поиск»

1. Общие положения

1.1. Настоящее поручение на обработку персональных данных Государственного автономного образовательного учреждения дополнительного образования «Центр для одаренных детей «Поиск» (далее – Поручение) разработано в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. N 152-ФЗ "О персональных данных", Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. № Пр-1895.

1.2. Настоящее Поручение определяет требования по организации обработки персональных данных в информационной системе Государственного автономного образовательного учреждения дополнительного образования «Центр для одаренных детей «Поиск» (далее – Центр «Поиск») с целью обеспечения безопасности персональных данных субъектов Центра «Поиск».

1.3. Список лиц, допущенных к обработке персональных данных, утверждается приказом директора Центра «Поиск» (Приложение 1).

1.4. Оператором является каждый сотрудник Центра «Поиск», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной или неавтоматизированной обработки персональных данных.

1.5. Оператор несет персональную ответственность за свои действия.

1.6. Оператор в своей работе руководствуется настоящим Поручением, руководящими и нормативными документами ФСТЭК России, регламентирующими документами Центра «Поиск» по защите информации.

1.7. Методическое руководство работой Оператора осуществляется ответственным за обеспечение информационной безопасности.

1.8. Непосредственную ответственность за надлежащее выполнение Поручения всеми Операторами Центра «Поиск» несет директор Центра.

1.9. Настоящее Поручение является дополнением к действующим нормативным документам по вопросам обеспечения безопасности защищаемой информации в Центре «Поиск» и не исключает обязательного выполнения их требований.

1.10. Нарушение настоящего Поручения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Должностные обязанности

Оператор обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые определены функциональными обязанностями.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Надежно хранить и никому не передавать номерную печать и использовать ее только для опечатывания помещения.

2.5. При отсутствии визуального контроля за рабочей станцией блокировать доступ к компьютеру.

2.6. В случае возникновения внештатных или аварийных ситуаций в рамках возложенных функций принимать меры по ликвидации их последствий.

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью Центра «Поиск», а также для получений консультаций по вопросам информационной безопасности, обращаться к администратору информационной безопасности.

2.8. Для получения консультаций по вопросам работы и настройки элементов ИСПДн обращаться к администратору информационной безопасности.

Оператору запрещается:

2.9. Разглашать защищаемую информацию третьим лицам.

2.10. Использовать компоненты программного и аппаратного обеспечения информационной системы Центра «Поиск» в неслужебных целях.

2.11. Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

2.12. Самостоятельно устанавливать, тиражировать, или модифицировать программное и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

2.13. Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

2.14. Подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

2.15. Отключать (блокировать) средства защиты информации.

2.16. Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав Оператора по доступу к ИСПДн.

2.17. Осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц.

2.18. Записывать и хранить информацию, содержащую сведения ограниченного распространения, на неучтенных носителях информации.

2.19. Сообщать (или передавать) посторонним лицам личные электронные ключи и атрибуты доступа к ресурсам ИСПДн.

2.20. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с администратором информационной безопасности.

3. Организация парольной защиты

3.1. Работа Оператора с паролями должна осуществляться в соответствии с Инструкцией по организации парольной защиты.

3.2. Личный пароль доступа к элементам ИСПДн формируется Оператором самостоятельно.

3.3. Полная плановая смена паролей проводится не реже одного раза в 180 дней.

3.4. Правила ввода пароля:

– Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

– Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранения пароля:

– Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

– Запрещается сообщать другим лицам личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны своевременно сообщать администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего пользования

4.1. Работа в сетях общего пользования Оператора ИСПДн должна осуществляться в соответствии с Инструкцией по обеспечению защиты информации при взаимодействии пользователей с информационными сетями общего пользования.

4.2. При работе в Сети запрещается:

– осуществлять работу при отключенных средствах защиты (антивирус и других);

– передавать по Сети защищаемую информацию без использования средств защиты каналов связи;

– посещать сайты, содержание которых не связано с выполняемыми Оператором функциональными обязанностями.