Государственное бюджетное общеобразовательное учреждение лицей №373 Московского района Санкт-Петербурга «Экономический лицей»

ПРИКАЗ

31.08.2022 **203-од**

О мерах, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом Российской Федерации «О персональных данных» в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей)

В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ

1. Утвердить:
   1.1. Правила обработки персональных данных в лицее согласно приложению №1.
   1.2. Порядок доступа сотрудников лицея в помещения, в которых ведется обработка персональных данных, согласно приложению № 2.
   1.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами Российской Федерации и организационно-распорядительными актами лицея согласно приложению №3.
   1.4. Правила работы с обезличенными данными согласно приложению №4.
   1.5. Правила рассмотрения запросов субъектов персональных данных или их представителей согласно приложению № 5.
   1.6. Инструкцию о действиях лиц, допущенных к информации, содержащей персональные данные, в случае возникновения нештатных ситуаций в лицее согласно приложению № 6.
   1.7. Инструкцию по порядку учета и хранению съемных машинных носителей информации, доступ к которой ограничен в соответствии с федеральными законами, в лицее согласно приложению № 7.
   1.8. Инструкцию о порядке резервного копирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и

средств защиты информации информационных систем персональных данных в лицее согласно приложению № 8.

1.9. Инструкцию ответственного за обработку персональных данных в лицее согласно приложению № 9.

1.10. Инструкцию пользователя персонального компьютера при работе в локальной вычислительной сети лицея согласно приложению № 10.

1.11. Инструкцию пользователя автоматизированной системы обработки конфиденциальной информации и персональных данных в лицее согласно приложению №11.

1.12. Инструкцию по организации антивирусной защиты в лицее согласно приложению № 12.

1.13. Перечень информационных систем персональных данных лицея, в которых должна быть обеспечена безопасность информации, согласно приложению № 13.

1.14. Перечень должностей сотрудников лицея ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных согласно приложению № 14.

1.15. Перечень сведений конфиденциального характера, подлежащих защите в лицее, согласно приложению № 15.

1.16. Перечень сотрудников лицея, допущенных к работе с персональными данными, обрабатываемыми согласно приложению № 16.

1.17. Форму согласия на обработку персональных данных согласно приложению № 17.

1.18. Форму обязательства сотрудника лицея непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (трудового договора) прекратить обработку персональных данных, ставших известными ему в связи исполнения должностных обязанностей, согласно приложению № 18.

1.19. Перечень защищаемой информации, обрабатываемой в лицее согласно приложению № 19.

1.20. Политика в отношении обработки персональных данных обработки персональных данных в лицее согласно приложению 20.

2. Назначить ответственным за организацию обработки персональных данных в лицее заместителя директора по УВР ***Кудрявцеву Ольгу Станиславовну***
3. Контроль за выполнением приказа оставляю за собой.

Директор лицея

Подписано цифровой подписью:
Афанасьева Ирина Викторовна
Дата: 2022.08.31 17:41:01 +03'00'

Приложение 1
к приказу
от 31.08.2022 №203-од

ПРАВИЛА
обработки персональных данных
в Государственном бюджетном общеобразовательном учреждении лицее №373
Московского района Санкт-Петербурга «Экономический лицей»
(далее – лицей)

Общие положения

1.1. Настоящие правила обработки персональных данных (далее – Правила) в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей) определяют цели, содержание и порядок обработки персональных данных (далее – ПДн), меры, направленные на защиту ПДн, а также мероприятия, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области ПДн при предоставлении услуг и обеспечения кадрового учета и бухгалтерской деятельности в лицее.

1.2. Настоящие Правила определяют политику лицея как оператора, осуществляющего обработку ПДн, в отношении обработки и защиты ПДн.

1.3. В целях настоящих Правил используются следующие понятия:

– Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники

– Блокирование ПДн – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

– Информационная система персональных данных (далее – ИСПДН) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;

– Конфиденциальность ПДн – обязанность оператора и иных лиц, получивших доступ к ПДн, не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом;

– Обезличивание ПДн – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;

– Обработка ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

– Оператор ПДн - самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку ПДн, а также определяющий цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн при предоставлении государственных и муниципальных услуг и обеспечения кадрового учета и бухгалтерской деятельности;

– ПДн – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

– Предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

– Распространение ПДн – действия, направленные на раскрытие ПДн неопределенному кругу лиц;

– Уничтожение ПДн – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

1.4. Настоящие Правила разработаны в соответствии:

– Трудовым кодексом Российской Федерации;

– Налоговым кодексом Российской Федерации;

– Кодексом Российской Федерации об административных правонарушениях;

– Федеральным законом от 27 июля 2006 г. (с изменениями на 14 июля 2022 года) № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

– Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральным законом от 27 июля 2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (далее – Федеральный закон «Об организации предоставления государственных и муниципальных услуг»);

– Федеральным законом от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации»;

– постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– постановлением Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

– постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.5. Обработка ПДн в лицее осуществляется с соблюдением порядка и условий, предусмотренных настоящими Правилами и законодательством Российской Федерации в области ПДн.

1.6. В лицее ведется обработка ПДн следующих категорий субъектов ПДн:

– физические лица, обратившиеся в лицей с целью получения государственных и муниципальных услуг, и их представителей;

– физические лица, обработка ПДн которых необходима для предоставления государственных и муниципальных услуг;

– индивидуальные предприниматели (далее – ИП) и физические лица – представители юридических лиц, фигурирующие в договорах, контрактах, жалобах;

– физические лица, претендующие на замещение должностей в лицее;

– сотрудники лицея.

2. Условия и порядок обработки ПДн физических лиц в связи с предоставлением государственных и муниципальных услуг

2.1. Обработка ПДн физических лиц, обратившихся в лицей для получения государственных и муниципальных услуг (далее – заявители), и их представителей осуществляется в целях организации предоставления государственных и муниципальных услуг, в том числе в электронной форме.

2.2. При организации предоставления государственных и муниципальных услуг заявителям и их представителям, их ПДн могут извлекаться для обработки из следующих документов, представляемых в форме документов на бумажном носителе или в форме электронных документов:

– документы, удостоверяющие личность гражданина Российской Федерации, в том числе военнослужащих, а также документы, удостоверяющие личность иностранного гражданина, лица без гражданства, включая вид на жительство и удостоверение беженца;

– документы воинского учета;

– свидетельства о государственной регистрации актов гражданского состояния;

– документы, подтверждающие регистрацию по месту жительства или по месту пребывания;

– документы на транспортное средство и его составные части, в том числе регистрационные документы;

– документы о трудовой деятельности, трудовом стаже и заработке гражданина, а также документы, оформленные по результатам расследования несчастного случая на производстве либо профессионального заболевания;

– документы о соответствующем образовании и (или) профессиональной квалификации, об ученых степенях и ученых званиях и документы, связанные с прохождением обучения, выдаваемые организациями, осуществляющими образовательную деятельность;

– справки, заключения и иные документы, выдаваемые организациями, входящими в государственную, муниципальную или частную систему здравоохранения;

– документы Архивного фонда Российской Федерации и другие архивные документы в соответствии с законодательством об архивном деле в Российской Федерации, переданные на постоянное хранение в государственные или муниципальные архивы;

– документы, выданные (оформленные) органами дознания, следствия либо судом в ходе производства по уголовным делам, документы, выданные (оформленные) в ходе гражданского судопроизводства либо судопроизводства в арбитражных судах, в том числе решения, приговоры, определения и постановления судов общей юрисдикции и арбитражных судов;

– решения, заключения и разрешения, выдаваемые органами опеки и попечительства в соответствии с законодательством Российской Федерации об опеке и попечительстве;

– правоустанавливающие документы на объекты недвижимости, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;

– документы, выдаваемые федеральными государственными учреждениями медико-социальной экспертизы;

– удостоверения и документы, подтверждающие право гражданина на получение социальной поддержки, а также документы, выданные федеральными органами исполнительной власти, в которых законодательством предусмотрена военная и приравненная к ней служба, и необходимые для осуществления пенсионного обеспечения лица в целях назначения и перерасчета размера пенсий;

– документы о государственных и ведомственных наградах, государственных премиях и знаках отличия;

– первичные статистические данные, содержащиеся в формах федерального статистического наблюдения, предоставленных юридическими лицами или индивидуальными предпринимателями;

– письменные уполномочия (доверенности) на обращение в лицей для получения государственных и муниципальных услуг от имени юридических и физических лиц выдаваемые другим физическим лицам.

2.3. В лицее подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан и лиц без гражданства, обратившихся в лицей лично в консультативных целях, а также направивших индивидуальные или коллективные письменные обращения или обращения в виде электронного документа, составленные в свободной форме.

2.4. В рамках рассмотрения обращений граждан Российской Федерации, иностранных граждан и лиц без гражданства подлежат обработке следующие ПДн, которые могут содержаться в обращениях:

– фамилия, имя, отчество (последнее при наличии);

– почтовый адрес;

– паспортные данные;

– адрес электронной почты;

– указанный в обращении контактный телефон;

– иные ПДн, указанные в обращении (жалобе).

2.5. ПДн, содержащиеся в обращениях, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением обратившихся лиц о результатах рассмотрения их обращений.

2.6. Для обработки ПДн заявителей, являющихся специальными ПДн, согласно пункту 1 части 2 статьи 10 Федерального закона «О персональных данных» и части 5 статьи 7 Федерального закона «Об организации предоставления государственных и муниципальных услуг» необходимо получение согласия в письменной форме.

2.7. Заявитель при обращении за предоставлением государственной или муниципальной услуги подтверждает факт получения указанного согласия в форме, предусмотренной законодательством Российской Федерации, в том числе путем представления документа, подтверждающего факт получения указанного согласия, на бумажном носителе или в форме электронного документа.

2.8. Согласие на обработку ПДн заполняется заявителями в соответствии с типовой формой согласия на обработку ПДн:

– согласие на ПДн данных может быть представлено в виде электронного документа, подписанного квалифицированной электронной подписью.

– согласие на обработку ПДн заявителя также может быть подано представителем заявителя, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя заявителя, полномочия данного представителя на дачу согласия от имени заявителя проверяются лицеем.

2.9. Для обработки ПДн лиц, не являющихся заявителями, обработка ПДн которых необходима для предоставления государственной или муниципальной услуги, на основании части 3 статьи 7 Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», необходимо получения согласия указанных лиц или их законных представителей в установленной форме.

2.10. Действие пункта 2.9 настоящих Правил не распространяется на лиц, признанных безвестно отсутствующими, и на разыскиваемых лиц, место нахождения которых не установлено уполномоченным федеральным органом исполнительной власти.

2.11. Обработка ПДн заявителей, необходимых для организации предоставления государственных и муниципальных услуг включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

2.12. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) ПДн заявителей для получения государственной услуги, осуществляется путем:

– получения оригиналов необходимых документов (заявление);

– заверения копий документов;

– внесения сведений в учетные формы (на бумажных и электронных носителях);

– внесения ПДн в прикладное программное обеспечение.

2.13. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) ПДн осуществляется путем получения ПДн непосредственно от заявителей или от их законных представителей.

2.14. При организации предоставления государственной услуги запрещается запрашивать у заявителей и третьих лиц ПДн, а также обрабатывать такие ПДн в случаях, не предусмотренных законодательством Российской Федерации.

2.15. При сборе ПДн сотрудники лицея осуществляющие получение ПДн непосредственно от заявителей, обязаны разъяснить указанным заявителям юридические последствия отказа предоставить ПДн. Форма разъяснения субъекту ПДн юридических последствий отказа представить свои ПДн в связи с предоставлением государственной и муниципальной услуги утверждается приказом директора.

2.16. Передача (предоставление, доступ) и использование ПДн заявителей осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

3. Условия и порядок обработки ПДн сотрудников лицея

3.1. ПДн сотрудников лицея обрабатываются в целях обеспечения кадровой и бухгалтерской деятельности в лицее, а также в целях обучения и должностного роста, учета результатов исполнения работниками должностных обязанностей, обеспечения им условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества.

3.2. В целях, предусмотренных пунктом 2.1 настоящих Правил, обрабатываются следующие категории ПДн сотрудников лицея:

– фамилия, имя отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

– серия и номер паспорта, кем и когда выдан;

– информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

– дата и место рождения;

– адрес прописки и проживания;

– телефонные номера (домашний, рабочий, сотовый);

– состояние в браке;

– ИНН и СНИЛС;

– трудовая деятельность до приема на работу;

– место работы и должность;

– период работы и данные о трудовом договоре;

– номер, серия и дата выдачи трудовой книжки;

– сведения о доходах и заработной плате;

– исполнительные листы;

– лицевые счета;

– сведения о контрагентах;

– сведения о квалификации и переподготовке;

– данные о повышении квалификации;

– наименование образовательного учреждения и документ, подтверждающий образование (номер, дата выдачи, специальность);

– ученая степень и звание;

– сведения о наличии специальных знаний или специальной подготовки;

– данные воинского учета;

– данные о наградах, медалях, поощрениях, почетных званиях;

– постановка на учет в ранние сроки беременности;

– временная нетрудоспособность;

– иные ПДн, необходимые для достижения целей, предусмотренных пунктом 3.1 настоящих Правил.

3.3 Обработка ПДн сотрудников лицея осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 3.1 настоящих Правил, в соответствии с пунктом 2 части 1 статьи 6 и частью 2 статьи 11 Федерального закона «О персональных данных», Трудовым кодексом Российской Федерации.

3.4 Обработка специальных категорий ПДн сотрудников лицея может осуществляться в рамках целей, определенных пунктом 3.1 настоящих Правил, в соответствии с подпунктом 2.3. пункта 2 части 2 статьи 10 Федерального закона «О персональных данных» и положениями Трудового кодекса Российской Федерации, за исключением случаев получения ПДн сотрудника у третьей стороны, при которых в соответствии с пунктом 3 статьи 86 Трудового кодекса Российской Федерации требуется письменное согласие.

3.5 Обработка ПДн сотрудников лицея осуществляется при условии получения от них письменного согласия на обработку ПДн в следующих случаях:

– при передаче (распространении, предоставлении) их ПДн третьим лицам, кроме случаев, предусмотренных действующим законодательством Российской Федерации;

– при принятии решений, порождающих юридические последствия в отношении сотрудников или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их ПДн.

3.6 В случаях, предусмотренных пунктом 3.5 настоящих Правил, согласие сотрудника на обработку его ПДн оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных». Форма согласия утверждается приказом директора.

3.7 Непосредственная обработка ПДн сотрудников лицея осуществляется специалистами Отдела бухгалтерского учета и отчетности, специалистами Отдела правового, кадрового, информационно-аналитического и организационного обеспечения.

3.8 Обработка ПДн сотрудников лицея включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

3.9 Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) ПДн сотрудников, а также граждан, претендующих на замещение должностей в лицее, осуществляется путем получения ПДн непосредственно от указанных лиц:

– получения оригиналов необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые в Отдел правового, кадрового, информационно-аналитического и организационного обеспечения;

– копирования оригиналов документов;

– внесения сведений в учетные формы (на бумажных и электронных носителях);

– формирования ПДн в ходе кадровой работы;

– внесения ПДн в ИСПДн, используемые Отделом правового, кадрового, информационно-аналитического и организационного обеспечения, а также Отделом бухгалтерского учета и отчетности.

3.10 В случае возникновения необходимости получения ПДн сотрудников, у третьей стороны, следует известить об этом сотрудника заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения ПДн.

3.11 Запрещается получать, обрабатывать и приобщать к личному делу сотрудника ПДн, не предусмотренные пунктом 3.2 настоящих Правил, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

3.12 При сборе ПДн сотрудник Отдела правового, кадрового, информационно-аналитического и организационного обеспечения, осуществляющий сбор (получение) ПДн

непосредственно от сотрудников, а также граждан, претендующих на замещение вакантных должностей в лицее, обязан разъяснить указанным субъектам ПДн юридические последствия отказа предоставить их ПДн.

3.13 Форма разъяснения субъекту ПДн юридических последствий отказа представить свои ПДн в связи с поступлением на работу и ее выполнением в лицее утверждается приказом директора.

3.14 Передача (распространение, предоставление) и использование ПДн сотрудников, а также граждан, претендующих на замещение вакантных должностей в лицее, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами

4 Порядок обработки ПДн субъектов ПДн в ИСПДн в лицее

4.1 Обработка ПДн субъектов ПДн осуществляется в ИСПДн Школы (далее АИС Школы), ИСПДн «ПараГраф 3», ИСПДн «Мониторинг обученности в системе общего образования «Знак»», ИСПДн «Профилактика правонарушений несовершеннолетних в ОУ Санкт-Петербурга», ИСПДн «Реестр по питанию», ИСПДн «База данных по проездным билетам учеников на общественном транспорте, база данных по проездным билетам учеников льготной категории».

4.2 АИСУ «ПараГраф 3», содержат ПДн сотрудников лицея, предусмотренные настоящими Правилами, и предназначены для обеспечения кадровой и бухгалтерской деятельности в лицее.

4.3 Классификация ИСПДн в лицее осуществляется в порядке, установленном законодательством Российской Федерации.

4.4 Сотрудниками лицея, имеющими право осуществлять обработку ПДн в ИСПДн, подписывается «Обязательство о неразглашении информации, содержащей персональные данные», по утвержденной приказом директора лицея форме.

4.5 Таким сотрудникам предоставляется уникальный логин и пароль для доступа к соответствующей ИСПДн. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными обязанностями сотрудников.

4.6 Информация с ПДн вносится в базы с ПДн и в другие места хранения информации в электронном виде в ручном режиме, при получении информации на бумажном носителе.

4.7 Обеспечение безопасности ПДн, обрабатываемых в ИСПДн, достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, а также принятия мер по обеспечению безопасности.

5 Сроки обработки и хранения ПДн в лицее

5.1 ПДн граждан, обратившихся в лицей лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в лицее до достижения целей обработки.

5.2 Заявления и соответствующие документы настоящих Правил, предоставляемые заявителями на бумажном носителе в связи с организацией предоставления государственных и муниципальных услуг, хранятся на бумажных носителях до достижения целей обработки.

5.3 ПДн, содержащиеся в приказах по личному составу (о приеме, о переводе, об увольнении, об установлении надбавок о поощрениях и т.д.), подлежат хранению в архиве лицея в течение 75 лет.

5.4 Документы, содержащие ПДн сотрудников, в том числе сведения о заработной плате, подлежат хранению в архиве лицея 75 лет.

5.5 ПДн при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на

разных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).

5.6 В лицее обеспечивается раздельное хранение ПДн на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящими Правилами.

5.7 Контроль хранения и использования материальных носителей ПДн, не допускающих несанкционированное использование, уточнение, распространение и уничтожение ПДн, находящихся на этих носителях, осуществляют руководители структурных подразделений, осуществляющих обработку ПДн субъектов ПДн

5.8 Срок хранения ПДн, внесенных в ИСПДн лицея, указанные в пунктах 4.1, 4.2 и 4.3 настоящих Правил, должен соответствовать сроку хранения бумажных оригиналов.

5.9 Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом «О персональных данных».

6. Порядок уничтожения ПДн при достижении целей обработки или при наступлении иных законных оснований

5.10 Ответственным за организацию обработки персональных данных в лицее осуществляется систематический контроль и выделение документов, содержащих ПДн, с истекшими сроками хранения и подлежащих уничтожению.

5.11 Вопрос об уничтожении выделенных документов, содержащих ПДн, рассматривается на заседании комиссии, состав которой утверждается приказом директора.

5.12 По итогам заседания составляются протокол и акт о выделении к уничтожению документов, опись уничтожаемых дел; дела проверяются на их комплектность, акт подписывается председателем и членами комиссии и утверждается директором.

5.13 Уничтожение документов, содержащих ПДн, производится членами комиссии путем сжигания или аппаратного измельчения.

5.14 По окончании процедуры уничтожения Ответственным за организацию обработки персональных данных в лицее составляется соответствующий акт об уничтожении документов, содержащих ПДн.

5.15 Уничтожение ПДн на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление ПДн, или программным удалением необходимой информации принятыми для конкретного типа носителя методами.

7. Ответственные за организацию обработки ПДн в Учреждении

7.1 Директором лицея назначается Ответственный за организацию обработки персональных данных, который курирует вопросы защиты информации в лицее. В полномочия Ответственного за организацию обработки персональных данных входит:

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

– организация внутренних проверок на предмет соблюдения сотрудниками требований законодательства Российской Федерации в области ПДн, в том числе требований к защите ПДн;

– инициирование разработки локальных актов по вопросам обработки ПДн, требований к защите ПДн;

– организация контроля приема и обработки обращений и запросов от субъектов ПДн;

– а случае нарушения в лицее требований к защите ПДн, принимать необходимые меры по восстановлению нарушенных прав субъектов ПДн.

7.2 Ответственный за организацию обработки ПДн, в соответствии с должностной инструкцией, вправе привлекать к реализации вышеуказанных мер по защите информации иных работников Учреждения с возложением на них соответствующих обязанностей и закреплением ответственности, а также вправе иметь доступ к информации, касающейся обработки ПДн и включающей:

– цели обработки ПДн;

– категории обрабатываемых ПДн;

– категории субъектов, ПДн которых обрабатываются;

– правовые основания обработки ПДн;

– перечень действий с ПДн, общее описание используемых в Учреждении способов обработки ПДн;

– описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

– дату начала обработки ПДн;

– срок или условия прекращения обработки ПДн;

– сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите ПДн, установленными Правительством Российской Федерации.

7.3 Непосредственное руководство работами, направленных на обеспечение защиты ПДн, а также контроль проводимых работ обеспечивает Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Учреждения, которому могут быть делегированы полномочия, перечисленные в пункте 7.2.

7.4 Ответственного за обеспечение безопасности персональных данных информационных систем персональных данных лицее согласно должностной инструкции участвует в разработке внутренних нормативных документов по защите ПДн.

7.5 Руководитель лицея несёт персональную ответственность за соблюдение установленного режима обработки ПДн субъектов ПДн.

7.6 Должностные лица, при проведении работ, связанных с обработкой ПДн, руководствуются законодательством Российской Федерации в области ПДн и настоящими Правилами.

7.7 Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, а также требований к защите ПДн, установленных Федеральным законом «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации.

7.8 Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПДн убытков.

Приложение 2
к приказу
от 31.08.2022 №203-од

ПОРЯДОК

доступа сотрудников Государственного бюджетного общеобразовательного учреждения лицея №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей) в помещения, в которых ведется обработка персональных данных

1. Общие положения

2.1. Настоящие порядок доступа (далее – Порядок) сотрудников лицея в помещения, в которых ведется обработка персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн), устанавливает единые требования к доступу сотрудников лицея в служебные помещения в целях предотвращения нарушения прав субъектов ПДн, обработка ПДн которых необходима для оказания государственных и муниципальных услуг и обеспечения кадровой и бухгалтерской деятельности в лицее, а также в целях обеспечения соблюдения требований законодательства РФ в области ПДн.

2.2. Настоящий Порядок разработан в соответствии с частью 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденных постановлением Правительства РФ от 21 марта 2012 г. № 211, и на основании «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденных приказом ФСТЭК России от 11 февраля 2013г. № 17, и «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных ФСБ России 21 февраля 2008 г. № 149/6/6-622.

2.3. Контролируемая зона (далее – контролируемая зона) – пространство (территория, здание, часть здания, помещение), в котором расположены средства автоматизации и защиты ИСПДн, в том числе автоматизированные рабочие места (далее – АРМ), на которых ведется обработка ПДн.

2.4. Перечень помещений, в которых ведется обработка ПДн, и их границы устанавливаются приказом лицея «Об определении границ контролируемой зоны и требований к ее безопасности».

2.5. Настоящий Порядок обязателен для применения и исполнения всеми сотрудниками лицея.

2.6. Ответственность за соблюдение положений настоящего Порядка несут сотрудники структурных подразделений лицея, обрабатывающие ПДн, а также руководители данных структурных подразделений.

2.7. Контроль соблюдения требований настоящего Порядка обеспечивает ответственный за организацию обработки ПДн в лицее.

2. Требования к помещениям контролируемой зоны

2.1. Бесконтрольный доступ сторонних лиц в помещения контролируемой зоны должен быть исключён.

2.2. Все помещения контролируемой зоны должны быть оборудованы охранной сигнализацией, либо предусматривать круглосуточное дежурство.

2.3. Ограждающие конструкции помещений контролируемой зоны должны предполагать существенные трудности для нарушителя по их преодолению.

2.4. К помещениям контролируемой зоны, в которых установлены криптографические средства защиты ПДн (далее – криптосредства) или хранятся ключевые

документы к ним, (далее – режимные помещения), предъявляются ужесточённые требования по безопасности, указанные в разделе 5 настоящих Правил.

3. Доступ в помещения контролируемой зоны

2.1. Доступ посторонних лиц в помещения контролируемой зоны, должен осуществляется только ввиду служебной необходимости.

2.2. На момент присутствия посторонних лиц в помещении контролируемой зоны, должны быть приняты меры по недопущению ознакомления посторонних лиц с ПДн (например: мониторы повёрнуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке или накрыты чистыми листами бумаги).

2.3. Допуск сотрудников в помещения контролируемой зоны оформляется после подписания сотрудником Обязательства о неразглашении информации, содержащей персональные данные, и инструктажа ответственным за организацию обработки ПДн в лицее, либо ответственным за обеспечение безопасности персональных данных информационных систем персональных данных лицея.

2.4. В нерабочее время помещения контролируемой зоны должны ставиться на охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты, материальные носители ПДн должны быть убраны в запираемые шкафы (сейфы), АРМ выключены или заблокированы.

4. Доступ в серверные помещения контролируемой зоны

2.1. Доступ в серверные помещения контролируемой зоны разрешён только администратору ИСПДн, ответственному за обеспечение безопасности персональных данных информационных систем персональных данных лицея и ответственному за организацию обработки ПДн в лицее.

2.2. Уборка серверных помещений происходит только при строгом контроле лиц, указанных в пункте 4.1 настоящих Правил

2.3. Серверные помещения контролируемой зоны в обязательном порядке оснащается охранной сигнализацией, системой видеонаблюдения и системой автономного питания средств охраны.

2.4. Доступ в серверные помещения контролируемой зоны посторонних лиц допускается строго по согласованию с ответственным за организацию обработки ПДн в лицее.

2.5. Нахождение в серверных помещениях контролируемой зоны посторонних лиц без сопровождающего не допустимо.

5. Требования к режимным помещениям

2.1. Режимные помещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

2.2. Размещение, специальное оборудование, охрана и организация режима в режимных помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

2.3. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.

2.4. Режимные помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять ответственному за организацию обработки ПДн в совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

2.5. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей должно быть предусмотрено необходимое число надёжных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у ответственного за организацию обработки ПДн в лицее.

2.6. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны.

2.7. Ключи от режимных помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ режимного помещения, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих режимных помещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за эти хранилища.

2.8. При утрате ключа от хранилища или от входной двери в режимное помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный за организацию обработки ПДн в лицее.

2.9. В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств или ответственным за организацию обработки ПДн в лицее. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за организацию обработки ПДн в лицее. Прибывший ответственный за организацию обработки ПДн в лицее должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.

2.10. Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

2.11. На время отсутствия пользователей криптосредств указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с ответственным за организацию обработки ПДн в лицее необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

Приложение 3
к приказу
от 31.08.2022 №203-од

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами Российской Федерации и организационно-распорядительными актами

1.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей) организуют проведение периодических проверок условий обработки персональных данных лицея.

1.2. Проверки осуществляются ответственным за организацию обработки персональных данных в лицее (далее - ответственный) либо комиссией, образуемой директором лицея.

1.3. В проведении проверки не может участвовать сотрудник (далее -сотрудник) лицея, прямо или косвенно заинтересованный в ее результатах.

1.4. Проверки соответствия обработки персональных данных лицея установленным требованиям к защите персональных данных проводятся на основании утвержденного ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в лицей письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки должно быть организовано директором лицея в течение трех рабочих дней с момента поступления соответствующего заявления.

1.5. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне определены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных; состояние учета машинных носителей персональных данных; соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.

1.6. Ответственный (комиссия) имеют право:

- запрашивать у сотрудников лицея 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 действующего законодательства Российской Федерации;
- вносить директору лицея предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить директору лицея предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации о персональных данных.

1.7. В отношении персональных данных, ставших известными главному ответственному (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

1.8. Проверка должна быть завершена не позднее чем через десять рабочих дней со дня принятия решения о ее проведении. О результатах проведенной проверки и мерах, необходимых для

устранения выявленных нарушений, директору лицея докладывает ответственный за организацию обработки данных либо председатель комиссии.

Приложение 4
к приказу
от 31.08.2022 №203-од

ПРАВИЛА
работы с обезличенными персональными данными
в Государственном бюджетном общеобразовательном учреждении лицее №373
Московского района Санкт-Петербурга «Экономический лицей»
(далее – лицей)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила работы с обезличенными персональными данными лицея разработаны с учетом Федерального закона от 27.07.2006 (с изм. от 14.07.2022) № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящие Правила определяют порядок работы с обезличенными данными лицея.

1.3. Настоящие Правила утверждаются директором лицея и действуют постоянно.

1.4. Настоящие Правила признаются утратившим силу на основании приказа.

1.5. Изменения в Правила вносятся приказом по лицею.

1.6. Изменения в Правила вносятся, в случаях: изменения законодательства Российской Федерации, изменения организационной структуры лицея, совершенствования системы информационной безопасности и т.п.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»:

2.1.1. Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

2.1.2. Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

2.1.3. Обезличивание персональных данных – действия, врезультате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

2.1.4. Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

2.1.5. Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели исодержание обработки персональных данных.

2.1.6. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц,

дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

2.1.7. Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

2.1.8. Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа кперсональным данным каким-либо иным способом.

2.1.9. Субъект - собственник информационных ресурсов (персональных данных), в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные. Субъект самостоятельно решает вопрос передачи своих персональных данных на основании согласия на обработку персональных данных.

3. УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ

3.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных лицея и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Способы обезличивания при условии дальнейшей обработкиперсональных данных:

3.2.1. уменьшение перечня обрабатываемых сведений;

абстрагирование ПД (сделать их менее точными, например путем группирования общих характеристик);

3.2.2. скрытие ПД (удаление всей или части записи ПД);

3.2.3. замена данных средним значением (замена выбранных данных средним значением для группы ПД);

3.2.4. разделение ПД на части (использование таблиц перекрестных ссылок);

3.2.5. маскирование ПД (замена одних символов в ПД другими);

3.2.6. замена части сведений идентификаторами;

3.2.7. обобщение, понижение точности некоторых сведений (сокращение сведений конкретизирующих субъект ПД);

3.2.8. деление сведений на части и обработка в разных информационных системах;

3.2.9. другие способы.

3.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

3.4. Для обезличивания персональных данных годятся любые способы,явно не запрещенные законодательно.

3.5. Работники, ответственные за проведение мероприятий по обезличиванию обрабатываемых персональных данных, директор, заместители директора.

3.5.1. Директор лицея принимает решение о необходимости обезличивания персональных данных;

3.5.2. Специалист, непосредственно осуществляющий обработку персональных данных «Оператор», готовит предложения по обезличиванию персональных данных,

обоснование такой необходимости и способ их обезличивания;

3.5.3. Специалист «Оператор», по согласованию с ответственным за обеспечение безопасности персональных данных осуществляетнепосредственное обезличивание выбранным способом.

4. ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

4.1. Обезличенные персональные данные относятся к 4-й категории (общедоступных) персональных данных, конфиденциальность для которых не обеспечивается. Доступ неограниченного круга лиц, к которым предоставляется с письменного согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

4.2. Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

4.2.1. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение порядка доступа в помещение, в котором ведется обработка персональных данных.

4.3. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- постановления Правительства Российской Федерации от 15 сентября2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации»;
- порядка доступа в помещения, в которых ведется обработка персональных данных.

Приложение 5
к приказу
от 31.08.2022 №203-од

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей

1.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей);
- правовые основания и цели обработки персональных данных;
  способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением сотрудников лицея), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с лицеем или на основании Закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом «О персональных данных»;
- сроки обработки персональных данных, в том числе сроки их хранения;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению директора лицея, если обработка поручена или будет поручена такому лицу.

1.2. Субъект персональных данных вправе требовать от лицея 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 действующим законодательством меры по защите его персональных данных.

1.3. Сведения должны быть предоставлены субъекту персональных данных лицеем в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

1.4. Сведения предоставляются субъекту персональных данных или его представителю лицеем по запросу.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с лицеем (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных лицеем, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

1.5. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в лицей или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее чем через тридцать дней после направления первоначального запроса, если более короткий срок не установлен Федеральном законом «О персональных данных».

1.6. Субъект персональных данных вправе направить повторный запрос в лицей в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 1.5 настоящих Правил, в случае если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального запроса. Повторный запрос наряду со сведениями, указанными в пункте 1.4, должен содержать обоснование направления повторного запроса.

1.7. Лицей вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 1.5 и 1.6. Такой отказ должен

быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на директоре лицея.

1.8. От имени субъекта персональных данных может выступать его представитель при наличии нотариально удостоверенной доверенности или доверенности приравненной к нотариально удостоверенной.

Приложение 6
к приказу
от 31.08.2022 №203-од

ИНСТРУКЦИЯ
о действиях лиц, допущенных к информации, содержащей персональные данные, в случае возникновения нештатных ситуаций в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей)

1. Общие положения

1.1. Настоящая инструкция определяет действия сотрудников (далее – сотрудники) лицея в случае возникновения нештатных ситуаций в процессе обработки персональных данных в информационных системах персональных данных (далее - ИСПДн).

1.2. Положения инструкции обязательны для исполнения всеми сотрудниками (работниками) в части выполнения вмененных им обязанностей.

1.3. Общими требованиями ко всем сотрудникам (работникам) в случае возникновения нештатной ситуации являются:

сотрудник (работник), обнаруживший нештатную ситуацию, немедленно ставит в известность администратора информационной безопасности;

администратор информационной безопасности (далее - администратор безопасности) обязан проводить анализ ситуации и, в случае невозможности исправить положение, ставит в известность директора лицея. Кроме этого, администратор безопасности для локализации (блокирования) проявлений угроз информационной безопасности может привлекать пользователей ИСПДн, а также уполномоченного сотрудника (работника), ответственного за сопровождение технических средств ИСПДн;

по факту возникновения нештатной ситуации и выяснению причин ее проявления проводится служебная проверка.

2. Действие пользователей ИСПДн при возникновении нештатных ситуаций

2.1. Сбой программного обеспечения.

2.1.1. Администратор безопасности совместно с сотрудником (работником) лицея (далее - сотрудник) выясняют причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультаций с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. О произошедшем инциденте администратор безопасности сообщает директору для принятия решения по существу.

2.2. Отключение электропитания технических средств ИСПДн.

2.2.1. Администратор безопасности совместно с сотрудником (работником) лицея проводят анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяют работоспособность оборудования. В случае необходимости производится восстановление программного обеспечения и данных из последней резервной копии с составлением акта. О произошедшем инциденте администратор безопасности сообщает директору лицея для принятия решения по существу.

2.3. Выход из строя технических средств ИСПДн (серверов, рабочих станций).

2.3.1. Сотрудник (работник) лицея совместно с администратором безопасности выполняют мероприятия по немедленному вводу в действие резервного сервера для обеспечения непрерывной работы ИСПДн (замене рабочей станции).

2.3.2. О выходе из строя сервера (рабочей станции) сотрудник (работник) лицея, ответственный за эксплуатацию сервера (рабочей станции), сообщает директору лицея.

2.3.3. При необходимости производятся работы по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.4. Потеря данных.

2.4.1. При обнаружении потери данных сотрудник (работник) (работник) лицея проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность программного обеспечения, целостность и работоспособность оборудования).

2.4.2. При необходимости сотрудник (работник) лицея производит восстановление программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте сотрудник (работник) лицея сообщает администратору безопасности. Администратор безопасности сообщает директору лицея для принятия решения по существу.

2.5. Обнаружение вредоносной программы в программной среде средств автоматизации ИСПДн.

2.5.1. При обнаружении вредоносной программы (далее - ВП) производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженная рабочая станция (сервер) физически отсоединяется от локальной вычислительной сети, и сотрудник (работник) лицея с администратором безопасности проводят анализ состояния рабочей станции (сервера).

2.5.2. В результате анализа может быть предпринята попытка сохранения данных, так как после перезагрузки рабочей станции (сервера) данные могут быть потеряны. После успешной ликвидации ВП сохраненные данные подвергаются повторной проверке на наличие ВП. Кроме того, при обнаружении ВП следует руководствоваться инструкцией по эксплуатации применяемого антивирусного программного обеспечения.

2.5.3. После ликвидации ВП проводится внеочередная проверка на всех средствах локальной вычислительной системы с применением обновленных антивирусных баз. При необходимости производится восстановление программного обеспечения и данных из резервных копий с составлением акта.

2.6. Утечка информации.

2.6.1. При обнаружении утечки информации ставится в известность администратор безопасности и директор лицея. По факту инициируется процедура служебной проверки. Если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов ИСПДн и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

2.7. Взлом операционной системы средств автоматизации ИСПДн (несанкционированное получение доступа к ресурсам операционной системы).

2.7.1. При обнаружении взлома сервера ставится в известность директор лицея.

2.7.2. По возможности производится временное отключение сервера от локальной вычислительной сети лицея для проверки на наличие ВП. Возможен временный переход на резервный сервер.

2.7.3. Сотрудником (работником) проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения. Сотрудником (работником) проводится анализ состояния файлов-скриптов и журналов сервера, производится смена всех паролей, которые имели отношение к данному серверу.

2.7.4. В случае необходимости сотрудником (работником) лицея производится восстановление программного обеспечения и восстановление данных из эталонного архива и резервных копий с составлением акта.

2.7.5. По результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в локальную вычислительную сеть, после чего проводятся аналогичные работы по проверке и восстановлению программного обеспечения и данных на других информационных узлах ИСПДн.

2.8. Попытка несанкционированного доступа (далее - НСД).

2.8.1. При попытке НСД сотрудником (работником) лицея и администратором безопасности проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД.

2.8.2. Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, сотрудником (работником) устанавливаются такие обновления.

2.8.3. В случае установления в ходе служебной проверки факта осуществления попытки НСД со стороны внешних по отношению к ИСПДн субъектов, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта-нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела.

2.9. Компрометация ключевой информации (паролей доступа).

2.9.1. При компрометации ключевой информации (пароля доступа) администратором безопасности проводится смена пароля, анализируется ситуация на наличие последствий компрометации и принимаются необходимые меры по минимизации возможного (или нанесенного) ущерба.

2.9.2. О произошедшем инциденте администратор безопасности сообщает директору лицея для принятия решения по существу.

2.10. Физическое повреждение или хищение оборудования технических средств ИСПДн.

2.10.1. Сотрудником (работником), обнаружившим физическое повреждение элементов ИСПДн, ставятся в известность директора лицея.

2.10.2. Сотрудником (работником) лицея совместно с администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов ИСПДн и возможные угрозы информационной безопасности.

2.10.3. О факте повреждения элементов ИСПДн сотрудник (работник) лицея докладывает директору лицея.

2.10.4. Сотрудником (работником) лицея проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.10.5. При необходимости сотрудником (работником) проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.11. Невыполнение установленных правил информационной безопасности (правил работы в ИСПДн), использование ИСПДн с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации.

2.11.1. Сотрудником (работником), обнаружившим невыполнение установленных правил ИБ, использование ИСПДн с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации, ставятся в известность: директор лицея и администратор безопасности.

2.11.2. Администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности (далее - ИБ) в результате инцидента.

2.11.3. Об обнаруженном факте администратор безопасности докладывает директору лицея.

2.12. Ошибки сотрудников (работников).

2.12.1. В случае возникновения сбоя, связанного с ошибками сотрудников (работником), руководитель подразделения, в котором произошел инцидент, ставит в известность уполномоченного сотрудника.

2.12.2. Администратором безопасности и сотрудником (работником) лицея проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента и необходимость восстановления программного обеспечения и данных.

2.12.3. При необходимости сотрудником (работником) проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.13. Отказ в обслуживании.

2.13.1. Сотрудником (работником), обнаружившим отказ в обслуживании, ставятся в известность: директор лицея и администратор безопасности.

2.13.2. Сотрудником (работником) и администратором безопасности проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

2.13.3. Сотрудником (работником) проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.13.4. При необходимости, сотрудником (работником) проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.13.5. О причинах инцидента и принятых мерах сотрудник (работник) информирует директора лицея.

2.14. Несанкционированные изменения состава программных и аппаратных средств (конфигурации) ИСПДн.

2.14.1. В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) ИСПДн администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы ИБ в результате инцидента.

2.14.2. Сотрудником (работником) лицея проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта, а также (при необходимости) проверка на наличие компьютерных ВП.

2.14.3. Об инциденте администратор безопасности докладывает директору лицея.

2.15. Техногенные и природные проявления нештатных ситуаций.

2.15.1. При стихийном бедствии, пожаре или наводнении, грозящем уничтожению или повреждению информации (данных), сотруднику (работнику), обнаружившему факт возникновения нештатной ситуации надлежит:

немедленно оповестить других сотрудников (работников) и принять все меры для самостоятельной оперативной защиты помещения;

немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.);

немедленно сообщить своему руководителю структурного подразделения и администратору безопасности.

2.15.2. После оперативной ликвидации причин, вызвавших пожар или наводнение, назначается внутренняя комиссия по устранению последствий инцидента.

2.15.3. Комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.

Приложение 7
к приказу
от 31.08.2022 №203-од

ИНСТРУКЦИЯ
по порядку учета и хранению съемных машинных носителей информации, доступ к которой ограничен в соответствии с федеральными законами в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей)

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» и другими нормативными правовыми актами, и устанавливает порядок использования съемных машинных носителей информации доступ, к которой ограничен в соответствии с федеральными законами, предоставляемых лицею для использования в информационных системах.

2. Основные термины, определения и сокращения

2.1. Администратор безопасности ЛВС лицея – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники (далее - администратор).

2.2. АРМ автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.

2.3. ИБ - информационная безопасность - комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

2.4. ИС - информационная система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

2.5. Съемный машинный носитель информации - материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемых с помощью средств вычислительной техники.

2.6. ПК - персональный компьютер.

2.7. Паспорт ПК - документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

2.8. ПО - программное обеспечение вычислительной техники.

2.9. ПО вредоносное - ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

2.10. ПО коммерческое - ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

2.11. Пользователь - сотрудник лицея, использующий мобильные устройства и машинные носители информации для выполнения своих служебных обязанностей.

3. Порядок использования съемных машинных носителей информации, доступ к которой ограничен в соответствии с федеральными законами (далее - машинные носители информации)

3.1. Под использованием машинных носителей информации в АИС Параграф понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и машинными носителями информации.

3.2. В ИС допускается использование только учтенных машинных носителей информации, которые являются собственностью лицея и подвергаются регулярной ревизии и контролю.

3.3. К предоставленным лицею машинным носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администратором безопасности).

3.4. Машинные носители информации предоставляются пользователям АИС Параграф по инициативе руководителей структурных подразделений в случаях:

необходимости выполнения вновь принятым пользователем своих должностных обязанностей;

возникновения у пользователей АИС Параграф производственной необходимости.

4. Порядок учета, хранения и обращения с машинными носителями информации, твердыми копиями и их утилизации

4.1. Все находящиеся на хранении и в обращении машинные носители информации в лицее подлежат учету.

4.2. Каждый машинный носитель информации с записанной на нем информацией должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу машинных носителей информации осуществляет администратор. Факт выдачи машинного носителя информации фиксируется в журнале учета машинных носителей информации. При увольнении пользователь сдает машинный носитель информации для хранения уполномоченному должностному лицу лицея, о чем делается соответствующая запись в журнале учета.

4.4. Пользователи могут получать машинный носитель от уполномоченного должностного лица лицея для выполнения работ на конкретный срок. При получении и сдаче машинного носителя делаются соответствующие записи в журнале учета.

4.5. При использовании пользователями машинных носителей информации необходимо:

4.5.1. Соблюдать требования настоящей Инструкции.

4.5.2. Использовать машинные носители информации исключительно для выполнения своих служебных обязанностей.

4.5.3. Ставить в известность администраторов о любых фактах нарушения требований настоящей Инструкции.

4.5.4. Бережно относиться к машинным носителям информации.

4.5.5. Обеспечивать физическую безопасность машинных носителей информации всеми разумными способами, в том числе хранением носителя в сейфе.

4.5.6. Извещать администраторов о фактах утраты (кражи) машинных носителей информации.

4.6. При использовании машинных носителей информации запрещено:

4.6.1. Использовать машинные носители информации в личных целях.

4.6.2. Передавать машинные носители информации другим лицам (за исключением администраторов).

4.6.3. Хранить машинные носители информации вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

4.6.4. Выносить машинные носители информации из служебных помещений для работы с ними на дому либо в других помещениях (местах).

4.7. Любое взаимодействие (обработка, прием, передача информации), инициированное пользователем между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администраторами заранее). Администратор оставляет за собой право блокировать или ограничивать использование машинных носителей информации.

4.8. Информация об использовании пользователем машинных носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена ответственному лицу в лицее за обработку персональных данных в лицее.

4.9. В случае выявления фактов несанкционированного и/или нецелевого использовании машинных носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой утвержден директором лицея.

4.10. По факту выясненных обстоятельств составляется акт расследования инцидента и передается директору лицея для принятия мер согласно действующему законодательству.

4.11. Информация, хранящаяся на машинных носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

4.12. При отправке или передаче информации адресатам на машинные носители информации записываются только предназначенные адресатам данные. Отправка информации адресатам на машинных носителях информации осуществляется в порядке, установленном для документов для служебного пользования.

4.13. Вынос машинных носителей информации для непосредственной передачи адресату осуществляется только с письменного разрешения администратора безопасности.

4.14. В случае утраты или уничтожения машинных носителей информации либо разглашении содержащихся в них сведений, об этом немедленно ставится в известность администратор безопасности. По факту утраты носителя составляется акт. Соответствующие отметки вносятся в журналы учета машинных носителей информации.

4.15. Машинные носители информации, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение машинных носителей информации осуществляется уполномоченной комиссией. По результатам уничтожения машинных носителей информации составляется акт согласно приложению к инструкции.

4.16. В случае увольнения или перевода пользователя в другое структурное подразделение, предоставленные ему машинные носители информации изымаются.

5. Ответственность

5.1. Пользователи, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством.

Приложение
к Инструкции по порядку учета и хранению
машинных носителей информации, доступ к

которой ограничен в соответствии с федеральными законами в лицее

АКТ[1]
об уничтожении (машинных, бумажных) носителей информации, доступ к которой ограничен в соответствии с федеральными законами

Комиссия в составе:
Председатель - _____
Члены комиссии - _____

провела отбор (машинных, бумажных) носителей информации, доступ к которой ограничен в соответствии с федеральными законами и установила, что в соответствии с требованиями руководящих документов по защите информации
_____ информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Кол-во	Примечание

Всего (машинных, бумажных) носителей

_____
(цифрами и прописью)

На указанных носителях информация, доступ к которой ограничен в соответствии с федеральными законами уничтожена путем

_____
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные материальные носители информации, доступ к которой ограничен в соответствии с федеральными законами уничтожены путем

_____
(разрезания, сжигания, механического уничтожения и т.п.)

Председатель комиссии: _____ / _____/

Члены комиссии: _____ / _____/

Приложение 8
к приказу
от 31.08.2022 №203-од

[1]**Примечание:**
1. Акт составляется раздельно на каждый способ уничтожения машинных носителей.
2. Все листы акта, а также все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.

ИНСТРУКЦИЯ
о порядке резервного копирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей)

1. Назначение и область действия

Порядок резервного копирования и восстановления работоспособности технических средств (далее - ТС) и программного обеспечения (далее - ПО), баз данных и средств защиты информации (далее - СЗИ) определяет действия (далее – Инструкция), связанные с функционированием информационных систем персональных данных (далее - ИСПДн) в лицее, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех сотрудников лицея (далее - пользователи), имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

Ответственным за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности ИСПДн лицея.

Ответственным за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных лицея.

2. *Порядок реагирования на инцидент*

В настоящем документе под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

В кратчайшие сроки, не превышающие одного рабочего дня, администратор безопасности ИСПДн и оператор ИСПДн предпринимают меры по восстановлению работоспособности информационной системы. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

системы жизнеобеспечения;

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

пожарные сигнализации и системы пожаротушения;

системы вентиляции и кондиционирования;

системы резервного питания.

Все критичные помещения лицея (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

резервные линии электропитания в пределах комплекса зданий;

аварийные электрогенераторы;

системы обеспечения отказоустойчивости;

кластеризация;

технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.2 Организационные меры

Резервное копирование и хранение данных должно осуществляться на периодической основе:

для обрабатываемых персональных данных - не реже раза в неделю; для технологической информации - не реже раза в месяц;

эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн - не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведении процедуры резервного копирования, должны отражаться в специально созданном журнале учета согласно приложению.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

4. Ответственность

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения резервного копирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных возлагается на администратора безопасности ИСПДн лицея.

Приложение

к Инструкции о порядке резервного копированиями и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в лицее

ЖУРНАЛ
учета записей резервных копий

№ записи	ИСПДн	Дата создания резервной копии	Наименование носителя	ФИО, должность лица, осуществившего резервное копирование	Подпись должностного лица, осуществившего резервное копирование

Приложение 9

к приказу
от 31.08.2022 №203-од

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей)

1. Инструкция ответственного за организацию обработки персональных данных (далее - Инструкция) разработана в соответствии с Федеральным законом «О персональных данных», Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», другими нормативными правовыми актами.

2. Инструкция определяет ответственность, обязанности и права лица, назначенного ответственным за организацию обработки персональных данных.

3. Ответственный за организацию обработки персональных данных отвечает за осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, доведение до сведений сотрудников лицея (далее - сотрудники) положений законодательства Российской Федерации о персональных данных, правовых актов лицея по вопросам обработки персональных данных, требований к защите персональных данных, организации приема и обработки обращений и осуществлению контроля за приемом и обработкой таких обращений.

4. Ответственный за организацию обработки персональных данных обязан:

— определить порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
— определять порядок и условия применения средств защиты информации;
— анализировать эффективность применения мер по обеспечению безопасности персональных данных;
— контролировать состояние учета машинных носителей персональных данных;
— проверять соблюдение правил доступа к персональным данным;
— контролировать проведение мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
— обеспечивать конфиденциальность персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля.

5. Ответственный за организацию обработки персональных данных имеет право:

— осуществлять проверки по контролю соответствия обработки персональных данных требованиям к защите персональных данных;
— запрашивать у сотрудников (работников) информацию, необходимую для реализации полномочий;
— требовать от ответственных за обработку персональных данных уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
— применять меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
— вносить директору лицея предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
— вносить директору лицея предложения о привлечении к дисциплинарной ответственности сотрудников (работников) лицея, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

Приложение 10
к приказу
от 31.08.2022 №203-од

ИНСТРУКЦИЯ
пользователя персонального компьютера при работе в локальной вычислительной сети в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей)

1. Общие положения

Целью настоящей Инструкции является регулирование работы пользователей персональных компьютеров при работе в локальной вычислительной сети лицея (далее - сеть), а также распределении сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа. Инструкция содержит необходимые требования по обеспечению совместной работы, более эффективному использованию сетевых ресурсов и уменьшению риска неправомерного их использования.

1.1. Сотруднику лицея (далее - пользователь) разрешена работа только на определенных компьютерах, в определенное регламентом время и только с разрешенными программами и сетевыми ресурсами.

1.2. Пользователь подключенного к сети компьютера - лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю прав доступа к компьютеру;

1.3. Каждый пользователь использует индивидуальное «имя пользователя» для своей идентификации в сети, выдаваемое службой технической поддержки в соответствии с заявкой.

1.4. Каждый пользователь самостоятельно задает пароль для входа в компьютерную сеть. При этом пароль должен содержать не менее 6 символов и состоять из букв и цифр. Рекомендации по использованию пароля приведены в Приложении к настоящей Инструкции.

1.5. Каждый пользователь должен использовать только свое имя пользователя и пароль для входа в компьютер, локальную сеть и сеть Интернет (если данный ресурс подключен). Передача имени пользователя и пароля третьим лицам, за исключением специалистов лицея для решения служебных задач, категорически запрещена.

1.6. В случае появления у пользователя сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере, или на каком-либо другом, пользователь должен немедленно сообщить об этом сотруднику (работнику), назначенному ответственным за защиту информации (далее - специалист, ответственный за защиту информации).

1.7. Специалист, ответственный за защиту информации, - лицо, следящее за правильным функционированием сети и комплексной защитой обрабатываемой информации. Специалист, ответственный за защиту информации, вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на обеспечение безопасности информации и повышение эффективности использования сетевых ресурсов.

1.8. Специалист, ответственный за защиту информации, имеет право отключить компьютер пользователя от сети в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, и в случаях других серьезных нарушений настоящей инструкции.

1.9. Специалист информирует пользователей, посредством уведомления через электронную почту, обо всех плановых профилактических работах, которые могут привести к частичной или полной неработоспособности сети на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам сети;

1.10. Пользователь должен ознакомиться с настоящей Инструкцией. Обязанность ознакомления пользователя с Инструкцией лежит на специалисте, ответственном за защиту информации.

2. Работа за компьютером

2.1. Запрещено самостоятельно вскрывать компьютер и вынимать его комплектующие. При возникновении неисправностей необходимо обратиться в службу технической поддержки.

2.2. Все кабели, соединяющие системный блок с другими устройствами, следует вставлять (вынимать) только при выключенном компьютере. Исключение составляют USB-устройства, они могут быть подключены к включенному компьютеру.

2.3. Запрещено самостоятельно устанавливать, удалять, деактивировать и изменять программное обеспечение на компьютере.

2.4. Запрещено аварийно завершать работу компьютера кнопкой «Reset» или отключением от электросети. Необходимо корректно завершать работу компьютера, через кнопку «Пуск» в панели задач. В случае невозможности корректного завершения работы компьютера обращаться к специалисту.

2.5. Запрещено подвергать компьютер и периферийные устройства физическим, термическим и химическим воздействиям.

2.6. Перед началом работы пользователь должен:

- включить выключатель сетевого фильтра. При включении кнопка должна начать светиться;
- включить источник бесперебойного питания (ИБП) и выждать 5 секунд (если установлен ИБП);
- включить монитор (если выключен);
- включить компьютер кнопкой «Power». Дождаться загрузки операционной системы (ОС);
- войти в систему, используя свой личный логин и пароль.

2.7. По завершении рабочего дня компьютер необходимо выключить и обесточить, для этого пользователь должен:

- закрыть все открытые программы и документы, сохранив нужные изменения; с помощью меню «Пуск - Завершение работы» выключить компьютер и дождаться завершения работы; выключить монитор;
- выключить ИБП, нажав кнопку на передней панели (если установлен ИБП);
- выключить сетевой фильтр.

2.8. При отключении электроэнергии ИБП позволяет компьютеру оставаться в рабочем состоянии до 5-10 минут. При отключении электроэнергии в помещении пользователь должен в немедленном порядке провести выключение компьютера в соответствии с пунктом 2.7. Инструкции.

3. Общие правила работы в локальной вычислительной сети *лицея*

3.1. Пользователи сети обязаны:

3.1.1. Соблюдать правила работы в сети, оговоренные настоящей Инструкцией.

3.1.2. При доступе к внешним ресурсам сети, соблюдать правила, установленные в лицее, для используемых ресурсов.

3.1.3. При уходе с рабочего места, необходимо активизировать средства защиты от несанкционированного доступа к информации при помощи сочетания клавиш «Ctrl+Alt+Del» и выбрав пункт «Блокировка».

3.1.3. Немедленно сообщать специалисту об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции. В лицее проводится расследование указанных фактов и принимаются соответствующие меры.

3.1.4. Не разглашать известную конфиденциальную информацию (имя пользователя и пароль), необходимую для безопасной работы в сети.

3.1.5. Выполнять предписания специалиста, ответственного за защиту информации, направленные на обеспечение безопасности сети.

3.1.6. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться в службу технической поддержки.

3.2. Пользователи сети имеют право:

3.2.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции.

3.2.2. Обращаться за помощью к специалисту при решении задач с использованием ресурсов сети.

3.2.3. Вносить предложения по улучшению работы с тем или иным ресурсом.

3.3. Пользователям сети запрещено:

3.3.1. Использовать любые программы, не предназначенные для выполнения прямых служебных обязанностей.

3.3.2. Разрешать посторонним лицам пользоваться вверенным пользователю компьютером (кроме случаев подключения/отключения ресурсов, выполняемого специалистами службы технической поддержки по заявке, согласованной со специалистом).

3.3.3. Самостоятельно устанавливать или удалять установленные программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов.

3.3.4. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.

3.3.5. Вскрывать сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без согласования со специалистом, изменять настройки BIOS, а также производить загрузку рабочих станций с различных носителей информации.

3.3.6. Самовольно подключать компьютер к сети, а также изменять настройки сети компьютера. Подключение к сети оборудования, не принадлежащего лицею, категорически запрещено, так как создает угрозу безопасности информации.

3.3.7. Получать и передавать в сеть информацию, противоречащую действующему законодательству Российской Федерации, представляющую служебную или государственную тайну, а также конфиденциальную информацию, в том числе персональные данные.

3.3.8. Использовать иные формы доступа к информационно-телекоммуникационной сети «Интернет».

3.3.9. Попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе.

4. Работа с электронной почтой

4.1. Электронная почта предоставляется пользователю только для выполнения своих прямых служебных обязанностей по служебной записке директора школы. Использование ее в личных целях запрещено. Создание почтового ящика проводится службой технической поддержки по заявке, согласованной с директором.

4.2. Лицей оставляет за собой право получить доступ к электронной почте пользователей. Содержимое электронного письма не может быть раскрыто, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.

4.3. Исходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности.

4.4. Использование электронной почты третьими лицами запрещено.

4.5. В качестве клиентов электронной почты могут использоваться только согласованные почтовые программы.

5. Работа в информационно-телекоммуникационной сети «Интернет»

5.1. Доступ к информационно-телекоммуникационной сети «Интернет» для пользователей предоставляется по служебной записке директора лицея на выделенных для работы с Интернет ресурсом персональных компьютерах.

5.2. Пользователи используют поиск информации в информационно-телекоммуникационной сети «Интернет» только в случае, если это необходимо для выполнения своих должностных обязанностей.

5.3. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему санкций.

5.4. Пользователям, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство Российской Федерации.

5.5. Программное обеспечение, используемые для работы в информационно-телекоммуникационной сети «Интернет», должно быть согласовано с директором лицея.

5.6. При необходимости переноса рабочих материалов, полученных из информационно-телекоммуникационной сети «Интернет», на персональный компьютер пользователя, требуется их проверка при помощи антивирусных программ, согласно Инструкции лицея по антивирусной защите.

5.7. Пользователи, должны соблюдать эту политику после предоставления им доступа к информационно-телекоммуникационной сети «Интернет».

6. Ответственность

6.1. Пользователь отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники.

6.2. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в сети и за ее пределами.

6.3. За нарушение настоящей инструкции пользователь может быть отстранен от работы в сети.

Приложение
к Инструкции пользователя персонального компьютера при работе в локальной вычислительной сети лицея

РЕКОМЕНДАЦИИ
по использованию пароля

1. Пароль должен включать в себя алфавитно-цифровые символы. Рекомендуется использовать буквы латинского алфавита. Кроме алфавитно-цифровых символов разрешается использовать, например, символы знаков препинания.
2. Минимальная длина пароля не должна быть менее 6 (шести) символов.
3. Пароль меняется не реже 1 раза в 30 дней.
4. Разрешается не более 6 попыток неверного ввода пароля.
5. Последние 6 паролей не должны повторяться.
6. Пароль для подключения к локальной сети должен регулярно обновляться самим пользователем.
7. Смена пароля пользователя осуществляется после входа в систему под своей учетной записью при помощи комбинации клавиш - Ctrl+Alt+Delete, а затем нажатием кнопки «Смена пароля» и действий в соответствии с предлагаемым алгоритмом (Ввод старого пароля, ввод нового пароля и его подтверждение).

Приложение 11
к приказу
от 31.08.2022 №203-од

ИНСТРУКЦИЯ
пользователя автоматизированной системы обработки конфиденциальной информации и персональных данных в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей)

1. Общие положения

1.1. Настоящая Инструкция разработана для обеспечения защиты конфиденциальной информации, в том числе персональных данных, в автоматизированных системах, используемых в лицее.

Конфиденциальная информация - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.2. Наиболее вероятными каналами утечки информации для автоматизированных систем (далее - АС) являются:

- несанкционированный доступ к информации, обрабатываемой в автоматизированной системе;
- хищение технических средств, с хранящейся в них информацией, или отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

1.3. Работа с конфиденциальной информацией, персональными данными, а также со служебными документами ограниченного распространения (далее - информация ограниченного распространения), строится на следующих принципах:

принцип персональной ответственности - в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный сотрудник, выдача документов осуществляется под роспись;

принцип контроля и учета - все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

2. Обязанности сотрудников лицея, имеющих доступ к конфиденциальной информации

2.1. Сотрудники лицея (далее - работники), получившие доступ к конфиденциальной информации, обязаны хранить в тайне данные сведения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки информации немедленно информировать директора лицея, специалиста по защите информации.

Конфиденциальная информация не подлежит разглашению. Прекращение доступа к такой информации не освобождает сотрудника (работника) от взятых им обязательств по неразглашению сведений ограниченного распространения.

В случае оставления занимаемой должности сотрудник (работник) обязан вернуть все документы и материалы, относящиеся к деятельности лицея. В том числе отчеты, инструкции, переписку, списки сотрудников (работников), компьютерные программы, а также все прочие материалы и копии названных

материалов, имеющих какое-либо отношение к деятельности администрации, полученные в течение срока работы.

2.2. Сотрудники (работники) при работе с конфиденциальной информацией обязаны:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;

выполнять требования специалиста по защите информации, касающиеся обеспечения информационной безопасности;

знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;

хранить в тайне свой аутентификатор (пароль доступа в автоматизированную систему), а также информацию о системе защиты, установленной на АС;

использовать для работы, только учтенные съемные накопители информации (гибкие магнитные диски, карты памяти, компакт диски и т.д.);

контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления в службу технической поддержки и специалисту по защите информации, ответственному за антивирусную защиту автоматизированной системы;

немедленно ставить в известность директора школы;

в случае утери носителя с конфиденциальной информацией или при подозрении компрометации личных ключей и паролей;

нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к защищенной АС;

несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АС.

В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в автоматизированной системе технических средств защиты ставить в известность ответственного за техническое обслуживание и (или) ответственного за обслуживание программного обеспечения.

2.3. Ставить в известность сотрудников (работников) лицея при:

необходимости обновления антивирусных баз;

обновлении программного обеспечения;

проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации АС;

необходимости вскрытия системных блоков персональных компьютеров входящих в состав АС;

резервном копировании информации.

2.4. Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

Вынос ПЭВМ, на которой проводилась обработка конфиденциальной информации, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с директором лицея запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному за учет служебных документов ограниченного распространения структурного подразделения. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы.

ПЭВМ, используемые для работы с конфиденциальной информацией, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана монитора, не имеющими отношения к конкретно обрабатываемой информации сотрудниками.

2.5. Запрещается:

передавать, кому бы то ни было (в том числе родственникам) устно или письменно конфиденциальную информацию;

использовать конфиденциальную информацию при подготовке открытых публикаций, докладов, научных работ и т.д.;

выполнять работы с документами, содержащими конфиденциальную информацию на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя;

накапливать ненужную для работы конфиденциальную информацию, при работе с персональными данными, соблюдать сроки ее хранения;

передавать или принимать без расписки документы, содержащие конфиденциальную информацию и персональные данные;

оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие конфиденциальную информацию, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами.

использовать компоненты программного и аппаратного обеспечения АС подразделения в неслужебных целях;

самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;

осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;

записывать и хранить конфиденциальную информацию на неучтенных носителях информации (картах памяти и т.п.);

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

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок - ставить в известность специалистов лицея.

3. Ответственность

Сотрудник (работник) несет ответственность за соблюдение требований настоящей инструкции, а также других документов в области защиты информации.

За разглашение конфиденциальной информации, персональных данных, а также служебной тайны, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, сотрудники могут быть привлечены к дисциплинарной или иной, предусмотренной действующим законодательством ответственности.

Приложение 12
к приказу
от 31.08.2022 №203-од

ИНСТРУКЦИЯ
по организации антивирусной защиты
в Государственном бюджетном общеобразовательном учреждении лицее №373
Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей)

1. Общие положения

Настоящая Инструкция определяет требования к организации защиты информации, обрабатываемой на компьютерах в лицее от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников лицея (далее - сотрудник) за ее выполнением.

2. Установка и обновление антивирусных средств

2.1. К использованию на компьютерах сотрудников лицея допускаются только лицензионные антивирусные средства.

2.2. Установка и настройка средств антивирусного контроля на компьютерах осуществляется специалистом лицея.

2.3. Обновление средств антивирусного контроля осуществляется автоматически.

3. Применение средств антивирусного контроля

3.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Контроль информации на съемных носителях производится непосредственно перед ее использованием.

3.2. Все жесткие диски персональных компьютеров проверяются на наличие вирусов системой антивирусной защиты в автоматическом режиме не реже одного раза в неделю.

3.3. Файлы, помещаемые в электронный архив (на сервер), должны в обязательном порядке проходить антивирусный контроль.

3.4. Особое внимание следует обратить на недопустимость использования съемных носителей, принадлежащих лицам, временно допущенным к работе на компьютере в лицее (обучающиеся, участники совещаний, студенты-практиканты и т.п.). Работа этих лиц должна проводиться под непосредственным контролем сотрудника или ответственного за информационную безопасность, особенно если работа происходит с использованием ресурсов локальной вычислительной сети.

3.5. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник структурного подразделения самостоятельно должен провести внеочередной антивирусный контроль компьютера и сообщить специалисту.

4. Действия сотрудников (работников) при обнаружении компьютерного вирус

4.1. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники (работники) подразделений обязаны: приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов специалисту;

совместно с владельцем зараженных вирусом файлов специалисты службы технической поддержки должны провести анализ необходимости дальнейшего их использования;

провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов службы технической поддержки).

5. Контроль

5.1. Контроль за проведением мероприятий антивирусного контроля в локальной вычислительной сети лицея и соблюдение требований настоящей Инструкции осуществляется заместителем директора по АХР.

5.2. Периодический контроль за соблюдением положений настоящей инструкции возлагается на специалиста лицея.

Приложение 13
к приказу
от 31.08.2022 №203-од

ПЕРЕЧЕНЬ
информационных систем персональных данных информации (далее – ИСПДн) в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей), в которых должна быть обеспечена безопасность

№ п/п	Наименование ИСПДн (ее составной части)	Наименование объекта (полное и сокращенное) Отраслевая (ведомственная) принадлежность Адрес объекта	Исходные данные классификации ИСПДн по требованиям защиты информации									Примечание
			Категория персональных данных	Принадлежность персональных данных	Количество персональных данных, содержащихся в информационной системе	Типы угроз, актуальных для информационной	Масштаб	Степень возможного ущерба	Уровень значимости информации (УЗ)	Класс защищенности	Уровень защищенности	
1	АИС «Параграф»	ГБОУ лицей №373 Московского района Санкт-Петербурга 196084, Санкт-Петербург, Московский пр. 112 литера А,	иные	Персональные данные сотрудников оператора, обучающихся и их родителей (законных представителей)	Менее 100000	Угрозы 3 типа	объектовый	низкая	4-й	К-3	УЗ-3	
2	Транспортная база	ГБОУ лицей №373 Московского района Санкт-Петербурга 196084, Санкт-Петербург, Московский пр. 112 литера А,	иные	Персональные данные обучающихся	Менее 100000	Угрозы 3 типа	объектовый	низкая	4-й	К-3	УЗ-3	

3	Школьное питание	ГБОУ лицей №373 Московского района Санкт-Петербурга 196084, Санкт-Петербург, Московский пр. 112 литера А,	иные	Персональные данные обучающихся и их родителей (законных представителей)								Автоматическая обработка информации не производится
4	База правонарушений	ГБОУ лицей №373 Московского района Санкт-Петербурга 196084, Санкт-Петербург, Московский пр. 112 литера А,	иные	Персональные данные сотрудников оператора, обучающихся и их родителей (законных представителей)	Менее 100000	Угрозы 3 типа	объектовый	низкая	4-й	К-3	УЗ-3	
5	База военнообязанных	ГБОУ лицей №373 Московского района Санкт-Петербурга 196084, Санкт-Петербург, Московский пр. 112 литера А,	иные	Персональные данные сотрудников оператора, обучающихся и их родителей (законных представителей)	Менее 100000	Угрозы 3 типа	объектовый	низкая	4-й	К-3	УЗ-3	

6	Кадры	ГБОУ лицей №373 Московского района Санкт-Петербурга 196084, Санкт-Петербург, Московский пр. 112 литера А,	иные	Персональные данные сотрудников оператора								Автоматическая обработка информации не производится
7	Обращения граждан, в том числе ПОС	ГБОУ лицей №373 Московского района Санкт-Петербурга 196084, Санкт-Петербург, Московский пр. 112 литера А,	иные	Персональные данные субъектов, не являющихся сотрудниками оператора								Автоматическая обработка информации не производится
8	ФИС ФРДО	ГБОУ лицей №373 Московского района Санкт-Петербурга 196084, Санкт-Петербург, Московский пр. 112 литера А,	иные	Персональные данные обучающихся	Менее 100000	Угрозы 3 типа	объектовый	низкая	4-й	К-3	УЗ-3	

Приложение 14
к приказу
от 31.08.2022 №203-од

ПЕРЕЧЕНЬ

должностей сотрудников в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей), ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в лицее

1. Директор школы – Афанасьева И.В.
2. Заместитель директора по УВР – Картюшова А.В.
3. Заместитель директора по УВР – Кудрявцева О.С.
4. Заместитель директора по АХР – Корнеева Н.Г.
5. Руководитель ОДО – Чистякова О.О.
6. Документовед – Голубева Л.Е.
7. Учитель информатики – Медведева Л.А.

Приложение 15
к приказу
от 31.08.2022 №203-од

ПЕРЕЧЕНЬ
сведений конфиденциального характера, подлежащих защите в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей)

1. Информация персонального характера сотрудников лицея (далее - сотрудники):
биографические и опознавательные данные;
отзывы о служебной деятельности и аттестационные листы;
служебное положение;
семейное положение;
социальное положение;
образование, навыки, профессии;
финансовое положение (уровень и состав доходов);
состояние здоровья;
домашний адрес и телефон;
иные персональные данные и сведения о фактах, событиях и обстоятельствах частной жизни сотрудников лицея за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
2. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна), а также:
   - сведения о системе управления лицеем (применяемые формы, методы и способы управления, предметы и цели совещаний, заседаний руководства, факты ведения переговоров; сведения о лицах, принимающих решения, перспективные планы развития, модернизации и совершенствования структуры подразделения; проекты приказов, распоряжений и постановлений);
   - картографическая информация ограниченного доступа;
   - информация об информационно-телекоммуникационных системах, каналах связи, компьютерных сетях, средствах вычислительной техники, программных средствах (операционных системах, системах управления базами данных и другого общесистемного и программного обеспечения), системах связи, передачи данных, используемых для сбора, хранения, обработки и передачи информации ограниченного доступа;
   - сведения о системах защиты информации (средства, методы и способы защиты информации, а также коды и процедуры доступа к информационным сетям).
3. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с действующим законодательством Российской Федерации.
4. Сведения, составляющие коммерческую тайну предприятий, организаций и других хозяйствующих субъектов, с которыми лицей заключил финансовые договора, и ставшие известными сотрудникам (работникам) лицей в силу их служебной деятельности.
5. Сведения о разработке новых технологий и алгоритмов, оригинальных программ и новых технических решений до официальной публикации информации о них.

Приложение 16
к приказу
от 31.08.2022 №203-од

ПЕРЕЧЕНЬ
сотрудников лицея в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – лицей), допущенных к работе с персональными данными

№	Фамилия	Имя	Отчество	Должность
1	Аврова	Кайрыкан	Мамадалиевна	учитель
2	Александрова	Марина	Валентиновна	учитель
3	Амелехина	Ирина	Юрьевна	учитель
4	Андрюшина	Елена	Владимировна	учитель
5	Андрющенко	Ирина	Геннадьевна	учитель
6	Анненков	Роман	Викторович	заместитель директора по ВР
7	Бакланова	Вера	Николаевна	учитель
8	Башков	Артём	Валерьевич	учитель
9	Бирюкова	Вера	Дмитриевна	учитель
10	Борисова	Мария	Вадимовна	учитель
11	Бохан	Ирина	Николаевна	учитель
12	Бошнякович	Ольга	Игоревна	методист
13	Бронникова	Ольга	Георгиевна	учитель
14	Буленкова	Мария	Евгеньевна	учитель
15	Бутусова	Елена	Владимировна	учитель
16	Васильева	Эльвира	Васильевна	заместитель директора по УВР
17	Величутин	Дмитрий	Александрович	учитель
18	Галиева	Гульшат	Фаиловна	учитель
19	Глотова	Елена	Владимировна	учитель
20	Гукова	Евгения	Сергеевна	учитель
21	Далла	Ольга	Антоновна	методист
22	Дмитрук	Анастасия	Викторовна	психолог
23	Жайворонок	Тамара	Петровна	учитель
24	Жебровская	Ольга	Олеговна	учитель
25	Картюшева	Анна	Валерьевна	заместитель директора по УВР
26	Кезина	Елена	Витальевна	учитель
27	Киселева	Наталья	Станиславовна	психолог
28	Коврижина	Елена	Александровна	учитель
29	Козловская	Елена	Васильевна	учитель
30	Колесова	Мария	Андреевна	учитель
31	Комиссарова	Валентина	Борисовна	учитель
32	Котенкова	Ирина	Валериевна	учитель
33	Кудрявцева	Ольга	Станиславовна	заместитель директора по УВР
34	Кудряшова	Оксана	Леонидовна	учитель
35	Кутина	Татьяна	Юрьевна	учитель
36	Латышев	Николай	Николаевич	учитель
37	Листраткина	Ируте	Владо	учитель
38	Личман	Татьяна	Борисовна	учитель
39	Ляпустина	Ольга	Юрьевна	учитель
40	Маркова	Ольга	Андреевна	учитель

41	Медведева	Людмила	Анатольевна	учитель
42	Михайлова	Елена	Петрасовна	учитель
43	Никитина	Марина	Геннадьевна	учитель
44	Носырева	Светлана	Викторовна	учитель
45	Оболашвили	Елена	Сергеевна	учитель
46	Павленко	Марина	Геннадьевна	учитель
47	Петрова	Светлана	Геннадьевна	учитель
48	Самофалова	Татьяна	Александровна	учитель
49	Сарана	Анастасия	Игоревна	учитель
50	Серкин	Сергей	Иванович	учитель
51	Смолякова	Ирина	Владимировна	учитель
52	Соловьева	Ирина	Анатольевна	учитель
53	Строгонова	Екатерина	Владимировна	социальный педагог
54	Сычевская	Екатерина	Валерьевна	учитель
55	Троянова	Елена	Викторовна	учитель
56	Туммель	Екатерина	Макаровна	учитель
57	Федорова	Полина	Васильевна	учитель
58	Фонина	Евгения	Олеговна	заместитель директора по УВР
59	Фурсикова	Екатерина	Сергеевна	учитель
60	Харитонов	Александр	Сергеевич	учитель
61	Хижнякова	Елена	Николаевна	учитель
62	Черная	Елена	Валентиновна	учитель
63	Чистякова	Ольга	Олеговна	Руководитель ДОД
64	Шерстнёва	Светлана	Львовна	учитель
65	Шушунова	Наталья	Федоровна	учитель

Приложение 17
к приказу
от 31.08.2022 №203-од

Руководителю государственного бюджетного общеобразовательного учреждения лицей № 373 Московского района Санкт-Петербурга «Экономический лицей» **Афанасьевой Ирине Викторовне**

от_____
_____
_____
(фамилия, имя, отчество (последнее при наличии) полностью)

Адрес регистрации
_____
_____
_____
_____

Сведения о документе, удостоверяющем личность заявителя_____
серия _____№ _____
дата выдачи _____
кем выдан_____
_____

Контактные телефоны
_____

СОГЛАСИЕ
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящим я, _____, представляю Работодателю (оператору) Государственному бюджетному общеобразовательному учреждению лицею № 373 Московского района Санкт-Петербурга «Экономический лицей» (ОГРН 1027804894281, ИНН 7810152614), зарегистрированному по адресу: 196084, Санкт-Петербург, Московский пр., д. 112, лит. А, свои персональные данные в целях обеспечения соблюдения трудового законодательства и иных нормативно-правовых актов для заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений, отражения информации в кадровых документах, начисления заработной платы, исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование, представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС России, сведений в ФСС РФ, предоставления сведений в кредитную организацию для оформления банковской карты и перечисления на нее заработной платы, обеспечения моей личной безопасности, текущей трудовой деятельности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества работодателя.

Моими персональными данными является любая информация, относящаяся ко мне как к физическому лицу (субъекту персональных данных), указанная в трудовом договоре, личной карточке работника (унифицированная форма Т-2), трудовой книжке и полученная в течение срока действия настоящего трудового договора, в том числе: мои фамилия, имя, отчество, год, месяц, дата и место рождения, гражданство, документы, удостоверяющие личность, идентификационный номер налогоплательщика, номер страхового свидетельства

государственного пенсионного страхования, адреса фактического места проживания и регистрации по месту жительства, почтовые и электронные адреса, номера телефонов, фотографии, сведения об образовании, профессии, специальности и квалификации, семейном положении и составе семьи, сведения об имущественном положении, доходах, задолженности, занимаемых ранее должностях и стаже работы, воинской обязанности; сведения о трудовом договоре и его исполнении (занимаемые должности, существенные условия труда, сведения об аттестации, повышении квалификации и профессиональной переподготовке, поощрениях и наказаниях, видах и периодах отпуска, временной нетрудоспособности, социальных льготах, командировании, рабочем времени и пр.), а также о других договорах (индивидуальной, коллективной материальной ответственности, ученических, оказания услуг и т. п.), заключаемых при исполнении трудового договора. Кроме того, даю согласие на размещение на официальном сайте Государственного бюджетного общеобразовательного учреждения лицея № 373 Московского района Санкт-Петербурга «Экономический лицей» моих персональных данных, а именно:

- фотографии с подписью фамилии, имени, отчества;
- сведений об образовании и повышении квалификации;
- сведений о почетных званиях и наличии квалификационной категории;
- адреса электронной почты.

Своей волей и в своих интересах выражаю согласие на осуществление Работодателем (оператором) любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных целей, в том числе выражаю согласие на обработку без ограничения моих персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в т. ч. передачу), обезличивание, блокирование, уничтожение персональных данных при автоматизированной и без использования средств автоматизации обработке; запись на электронные носители и их хранение; передачу Работодателем (оператором) по своему усмотрению данных и соответствующих документов, содержащих персональные данные, третьим лицам: налоговым органам, в отделения Пенсионного фонда, Фонда социального страхования, Фонда обязательного медицинского страхования, банку ПАО «Банк Санкт-Петербург» в рамках зарплатного проекта; хранение моих персональных данных в течение 75 лет, содержащихся в документах, образующихся в деятельности Работодателя (оператора), согласно действующему законодательству Российской Федерации, а также при осуществлении любых иных действий с моими персональными данными, указанными в трудовом договоре и полученными в течение срока действия трудового договора, в соответствии с требованиями действующего законодательства РФ и Закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Настоящее согласие на обработку персональных данных действует с момента представления бессрочно и может быть отозвано мной при представлении Работодателю (оператору) заявления в простой письменной форме в соответствии с требованиями законодательства Российской Федерации.

Обязуюсь сообщать Государственному бюджетному общеобразовательному учреждению лицею № 373 Московского района Санкт-Петербурга «Экономический лицей» об изменении местожительства, контактных
телефонов, паспортных, документных и иных персональных данных. Об ответственности за достоверность представленных персональных сведений предупрежден(а).

"____"_____ 20___ года _____/_____/
подпись расшифровка

Приложение 18

к приказу
от 31.08.2022 №203-од

Руководителю государственного бюджетного общеобразовательного учреждения лицей № 373 Московского района Санкт-Петербурга «Экономический лицей» **Афанасьевой Ирине Викторовне**
от_____
_____
_____
(фамилия, имя, отчество (последнее при наличии) полностью)
Адрес регистрации
_____
_____
_____
_____
Сведения о документе, удостоверяющем личность заявителя_____
серия _____№ _____
дата выдачи _____
кем выдан_____
_____

Контактные телефоны
_____

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных

Я, _____, добровольно принимаю на себя обязательства:

– не разглашать и не передавать третьим лицам персональные данные работников, учащихся и их родителей (законных представителей), к которым я имею доступ в соответствии с трудовым договором, должностной инструкцией в связи с исполнением должностных обязанностей;

– не использовать конфиденциальные сведения о работниках, учащихся и их родителях (законных представителях) с целью получения выгоды. В случае попытки третьих лиц получить от меня конфиденциальные сведения сообщить об этом директору государственного бюджетного общеобразовательного учреждения лицей № 373 Московского района Санкт-Петербурга «Экономический лицей»;

– выполнять требования законодательства РФ и локальных актов государственного бюджетного общеобразовательного учреждения лицей № 373 Московского района Санкт-Петербурга «Экономический лицей», регламентирующих обработку персональных данных.

Мне известно, что в случае нарушения данного обязательства я буду привлечена к ответственности в соответствии с законодательством РФ.

"____"_____ 20___ года _____/_____/
подпись расшифровка

Приложение 19

к приказу
от 31.08.2022 №203-од

Перечень защищаемой информации, обрабатываемой в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей»

№ п\п	Наименование	Размещение	Основание для защиты
1	ПДн сотрудников	Сетевой программно-технологический комплекс «ПараГраф 3», Личные дела сотрудников	ФЗ №152-ФЗ «О персональных данных»
2	ПДн учащихся, ПДн родителей учащихся	Сетевой программно-технологический комплекс «ПараГраф 3», Автоматизированная информационная система «Мониторинг обученности в системе общего образования «Знак», Информационно-поисковая система «Профилактика правонарушений несовершеннолетних в ОУ Санкт-Петербурга», Реестр по питанию, База данных по проездным билетам учеников на общественном транспорте, База данных по проездным билетам учеников льготной категории, Классные журналы, Журналы ГПД, Журналы ПДО, Договора, Медицинские карты учащихся, Личные дела учащихся, Картотека соц. педагога	ФЗ №152-ФЗ «О персональных данных»
3	Технологическая информация, обрабатываемая в ЛВС ОУ	Сетевой программно-технологический комплекс «ПараГраф 3», Автоматизированная информационная система «Мониторинг обученности в системе общего образования «Знак»	Специальные требования и рекомендации по технической защите конфиденциальной информации.

Приложение 20

к приказу
от 31.08.2022 №203-од

ПОЛИТИКА
в отношении обработки персональных данных в Государственном бюджетном общеобразовательном учреждении лицее № 373 Московского района Санкт-Петербурга «Экономический лицей»

1. Общие положения

1.1. Назначение Политики

1.1.1. Политика в отношении обработки персональных данных в Государственном бюджетном общеобразовательном учреждении лицее №373 Московского района Санкт-Петербурга «Экономический лицей» (далее – Лицей, Оператор) (далее – Политика) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и определяет политику в отношении обработки персональных данных в Лицее, а также правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере 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.

1.1.2. Политика вступает в силу с момента ее утверждения директором Лицея.

1.1.3. Политика подлежит пересмотру в ходе периодического анализа, но не реже одного раза в год, ответственного за организацию обработки персональных данных в Лицее, а также в случаях изменения законодательства Российской Федерации в области персональных данных.

1.1.4. Политика подлежит опубликованию на официальном сайте Лицея (https://лицей373.рф/)

1.2. Цели Политики

1.2.1. Целью Политики является обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных Лицеем.

1.3. Основные понятия (термины, определения)

1.3.1. Для целей Политики используются следующие 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;

субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных;

оператор – государственный, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие 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) с персональными данными, совершаемых с использованием средств автоматизации или без их использования, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), 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;

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицами без согласия ее обладателя;

трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационных системах персональных данных;

уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

1.4. Область действия

1.4.1. Положения Политики распространяются на все отношения, связанные с обработкой персональных данных, осуществляемой Лицеем:

– с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным;

– без использования средств автоматизации.

1.4.2. Настоящей Политикой должны руководствоваться все сотрудники Лицея, осуществляющие обработку персональных данных или имеющие к ним доступ.

2. Цели обработки персональных данных

2.1. Обработка персональных данных осуществляется Лицеем в следующих целях:

- для исполнения условий трудового договора и осуществления прав и обязанностей в соответствии с трудовым законодательством;
- для принятия решения о трудоустройстве;
- для принятия решений по обращениям граждан Российской Федерации в соответствии с действующим законодательством;
- для исполнения обязанностей по гражданско-правовым договорам с Лицеем;
- для оказания государственных услуг, в том числе для наиболее полного исполнения Лицеем своих обязанностей, обязательств и компетенций, определенных действующим законодательством Российской Федерации.

3. Правовые основания обработки персональных данных

3.1. Основанием обработки персональных данных в Лицее являются:

- Конституция Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
- Федеральный закон от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;
- Федеральный закон от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;
- Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;
- Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системах обязательного пенсионного страхования и обязательного социального страхования»;
- Федеральный закон от 16.07.1999 № 165-ФЗ «Об основах обязательного социального страхования»;
- Федеральный закон от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе»;
- иные нормативные правовые акты, регулирующие отношения, связанные с деятельностью Лицея.

3.2. Правовым основанием обработки персональных данных также являются:

- Устав Лицея;
- договоры, заключаемые между Лицеем и субъектами персональных данных;
- согласие субъектов персональных данных на обработку их персональных данных.

3.3. В случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям Лицея, обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

3.3. Обработка персональных данных прекращается при реорганизации или ликвидации Лицея.

4. Категории субъектов персональных данных, категории и перечни обрабатываемых персональных данных в зависимости от цели обработки, способы и сроки их обработки и хранения.

4.1. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, предусмотренным в разделе 2 настоящей Политики. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.2. Оператор может обрабатывать персональные данные следующих категорий субъектов персональных данных:

4.2.1. Кандидаты для приема на работу к Оператору – для целей исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, осуществления пропускного режима:

• фамилия, имя, отчество;
• пол;
• гражданство;
• дата и место рождения;
• контактные данные;
• сведения об образовании, опыте работы, квалификации;
• иные персональные данные, сообщаемые кандидатами в резюме и сопроводительных письмах.

4.2.2. Работники и бывшие работники Оператора – для целей исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, осуществления пропускного режима:

• фамилия, имя, отчество;
• пол;
• гражданство;
• дата и место рождения;
• изображение (фотография);
• паспортные данные;
• адрес регистрации по месту жительства;
• адрес фактического проживания;
• контактные данные;
• индивидуальный номер налогоплательщика;
• страховой номер индивидуального лицевого счета (СНИЛС);
• сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации;
• семейное положение, наличие детей, родственные связи;
• сведения о трудовой деятельности, в том числе наличие поощрений, награждений и (или) дисциплинарных взысканий;
• данные о регистрации брака;
• сведения о воинском учете;
• сведения об инвалидности;
• сведения об удержании алиментов;
• сведения о доходе с предыдущего места работы;
• иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства.

4.2.3. Обучающиеся и их родители (законные представители) – для оказания государственных услуг, предусмотренных действующим законодательством Российской Федерации:

• фамилия, имя, отчество;
• пол;
• гражданство;

• дата и место рождения;
• изображение (фотография);
• паспортные данные (данные свидетельства о рождении);
• адрес регистрации по месту жительства;
• адрес фактического проживания;
• контактные данные;
• иные персональные данные, предоставляемые обучающимися и их родителями (законными представителями) в соответствии с требованиями действующего законодательства Российской Федерации.

4.2.4. Члены семьи работников Оператора – для целей исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений:
• фамилия, имя, отчество;
• степень родства;
• год рождения;
• иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства.

4.2.5. Контрагенты Оператора (физические лица) – для целей осуществления своей деятельности в соответствии с Уставом Лицея, осуществления пропускного режима:
• фамилия, имя, отчество;
• дата и место рождения;
• паспортные данные;
• адрес регистрации по месту жительства;
• контактные данные;
• замещаемая должность;
• индивидуальный номер налогоплательщика;
• номер расчетного счета;
• иные персональные данные, предоставляемые контрагентами (физическими лицами), необходимые для заключения и исполнения договоров.

4.2.6. Представители (работники) контрагентов Оператора (юридических лиц) – для целей осуществления своей деятельности в соответствии с Уставом Лицея, осуществления пропускного режима:
• фамилия, имя, отчество;
• паспортные данные;
• контактные данные;
• замещаемая должность;
• иные персональные данные, предоставляемые представителями (работниками) контрагентов, необходимые для заключения и исполнения договоров.

4.3. Оператор осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требует каждая цель обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором.

4.3.1. Персональные данные на бумажных носителях хранятся в Лицее в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ (Федеральный закон от 22.10.2004 N 125-ФЗ «Об архивном деле в Российской Федерации», Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения (утв. Приказом Росархива от 20.12.2019 № 236)).

4.3.2. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

4.4. Оператор прекращает обработку персональных данных в следующих случаях:
• выявлен факт их неправомерной обработки;

• достигнута цель их обработки;

• истек срок действия или отозвано согласие субъекта персональных данных на обработку указанных данных, когда в соответствии с Законом о персональных данных обработка этих данных допускается только с согласия.

4.5. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку Оператор прекращает обработку этих данных, если:

• иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

• Оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;

• иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

4.6. При обращении субъекта персональных данных к Оператору с требованием о прекращении обработки персональных данных в срок, не превышающий 10 рабочих дней с даты получения Оператором соответствующего требования, обработка персональных данных прекращается, за исключением случаев, предусмотренных Законом о персональных данных. Указанный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Оператору необходимо направить субъекту персональных данных мотивированное уведомление с указанием причин продления срока.

4.7. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

5. Порядок и условия обработки персональных данных

5.1. Принципы обработки персональных данных

Обработка персональных данных осуществляется Лицеем в соответствии со следующими принципами:

обработка персональных данных осуществляется на законной основе;

обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей; не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

обработке подлежат только персональные данные, которые отвечают целям их обработки;

содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки; обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки;

при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных; Лицей принимает необходимые меры (либо обеспечивает их принятие) по удалению или уточнению неполных или неточных данных;

хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных; обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки

или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.2. Условия обработки персональных данных

5.2.1. Условия обработки специальных категорий персональных данных

Оператор осуществляет обработку специальных категорий персональных данных, касающихся состояния здоровья.

Обработка специальных категорий персональных данных осуществляется Лицеем с соблюдений следующих условий:

обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных.

5.2.2. Условия обработки биометрических персональных данных

Обработка сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются для установления личности субъекта персональных данных, Лицеем не осуществляется.

5.2.3. Условия обработки иных категорий персональных данных

Обработка иных категорий персональных данных осуществляется Лицеем с соблюдением следующих условий:

обработка персональных данных необходима для достижения целей, предусмотренных действующим законодательством Российской Федерации, а также для осуществления и выполнения возложенных действующим законодательством на Лицей функций, полномочий и обязанностей;

обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

5.2.4. Поручение обработки персональных данных

5.2.4.1. Лицей вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта (далее – поручение).

5.2.4.2. Лицо, осуществляющее обработку персональных данных по поручению Лицея, соблюдает принципы и правила обработки персональных данных, предусмотренные настоящей Политикой, соблюдает конфиденциальность персональных данных, принимает необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных».
В поручении Лицея определяются: перечень персональных данных; перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных; способы и цели их обработки; установлена обязанность такого лица соблюдать конфиденциальность персональных данных; требования, предусмотренные частью 5 статьями 18 и 18.1 Федерального закона «О персональных данных»; обязанность по запросу Лицея в течение срока действия поручения лицея, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Лицея требований, установленных в соответствии с частью 3 статьи 6 Федерального закона «О персональных данных»; обеспечивать безопасность персональных данных при их обработке, а также указаны требования к защите обрабатываемых персональных данных, в том числе требование об уведомлении Лицея о случаях, предусмотренных частью 3.1 статьи 21 Федерального закона «О персональных данных».

5.2.4.3. При поручении обработки персональных данных другому лицу ответственность перед субъектом персональных данных за действия указанного лица несет Лицей. Лицо, осуществляющее обработку персональных данных по поручению Лицея, несет ответственность перед Лицеем.

5.2.5. Передача персональных данных

Передача персональных данных возможна при наличии письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в других случаях, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами Российской Федерации.

5.3. Конфиденциальность персональных данных

5.3.1. Работники Лицея, получившие доступ к персональным данным, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.4. Общедоступные источники персональных данных

Оператором созданы общедоступные источники персональных данных: официальный сайт Лицея.

5.5. Согласие субъекта персональных данных

5.5.1. При необходимости обеспечения условий обработки персональных данных субъекта может предоставляться согласие субъекта персональных данных на обработку его персональных данных.

5.5.2. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Лицеем.

5.5.3. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Лицей вправе продолжить обработку персональных данных без согласия субъекта персональных данных при выполнении условий обработки персональных данных, указанных в статье 6 ФЗ «О персональных данных».

5.5.4. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство выполнения условий обработки персональных данных, указанных в статье 6 ФЗ «О персональных данных», возлагается на Лицей.

5.5.5. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

– фамилию, имя, отчество, адрес места жительства (по паспорту, фактический) субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, код подразделения, выдавшего документ, удостоверяющий личность;

– фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование и адрес Лицея;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Лицея, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Лицеем способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

5.5.6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

5.5.7. Персональные данные могут быть получены Лицеем от лица, не являющегося субъектом персональных данных, при условии предоставления Лицею подтверждения наличия условий обработки информации, указанных в статье 6 Федерального закона «О персональных данных».

5.6. Трансграничная передача персональных данных

Трансграничная передача персональных данных Лицеем не осуществляется.

5.7. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения

5.7.1. Обработка персональных данных, разрешенных субъектом персональных данных для распространения, может осуществляться на основании соответствующего согласия субъекта персональных данных.

5.7.2. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

5.7.3. Согласие содержит перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

5.7.4. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, предоставляется непосредственно Лицею.

5.7.5. Молчание или бездействие субъекта персональных данных не считается согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

5.7.6. В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных Лицеем неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ Лицея в установлении субъектом персональных данных запретов и условий, предусмотренных статьей 10.1 Федерального закона «О персональных данных», не допускается.

5.7.7. Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

5.7.8. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только Лицеем.

5.7.9. Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления Лицею соответствующего требования.

5.7.10. Требования, указанные в п.п. 5.7 Политики, не применяются в случае обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на государственные органы, муниципальные органы, а также на подведомственные этим органам организации функций, полномочий и обязанностей.

5.8. Обработка персональных данных, осуществляемая без использования средств автоматизации

5.8.1. Общие положения

5.8.1.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

5.8.2. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

5.8.2.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

5.8.2.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных используется отдельный материальный носитель.

5.8.2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники Лицея или лица, осуществляющие такую обработку по договору с Лицеем), проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Лицеем без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Лицея.

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

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) содержат сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес Лицея, 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 Лицеем способов обработки персональных данных;

б) типовая форма предусматривает поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма составляется 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;

г) типовая форма исключает объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

5.8.2.5. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Лицей, или в иных аналогичных целях, соблюдаются следующие условия:

а) необходимость ведения такого журнала (реестра, книги) предусмотрена актом Лицея, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится Лицей, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится Лицей.

5.8.2.6. 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, принимаются меры по обеспечению раздельной обработки персональных данных, в частности:

а) 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;

б) 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.

5.8.2.7. Уничтожение 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). Указанные правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

5.8.2.8. 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.

5.8.3. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

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

5.8.3.2. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

5.8.3.3. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Лицеем.

5.9. Обработка метрических данных

На сайте Лицея (https://лицей373.рф/) применяется инструмент веб-аналитики Яндекс.Метрика. Инструмент веб-аналитики применяется в целях анализа использования сайта Лицея и улучшения его работы.

6. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

6.1. Права субъектов персональных данных

6.1.1. Право субъекта персональных данных на доступ к его персональным данным

6.1.1.1. Субъект персональных данных имеет право на получение информации (далее – запрашиваемая субъектом информация), касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных Лицея;

– правовые основания и цели обработки персональных данных;

– цели и применяемые Лицеем способы обработки персональных данных;

– наименование и место нахождения Лицея, сведения о лицах (за исключением работников лицея), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Лицеем или на основании федерального закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Лицея, если обработка поручена или будет поручена такому лицу;

– информацию о способах исполнения Лицеем обязанностей, установленных статьей 18.1 Федерального закона «О персональных данных»;

– иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

6.1.1.2. Субъект персональных данных имеет право на получение запрашиваемой субъектом информации, за исключением следующих случаев:

обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

6.1.1.3. Субъект персональных данных вправе требовать от Лицея 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.

6.1.1.4. Запрашиваемая субъектом информация должна быть предоставлена субъекту персональных данных Лицеем в доступной форме, и в ней не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6.1.1.5. Запрашиваемая информация предоставляется субъекту персональных данных или его представителю Лицеем в течение десяти рабочих дней с момента обращения либо получения Лицеем запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней, в случае направления Лицеем в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя; сведения о дате выдачи указанного документа и выдавшем его органе; сведения, подтверждающие участие субъекта

персональных данных в отношениях с Лицеем (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения) либо сведения, иным образом подтверждающие факт обработки персональных данных Лицеем; подпись субъекта персональных данных или его представителя (далее – необходимая для запроса информация). Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Лицей предоставляет запрашиваемые сведения субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение или запрос, если иное не указано в обращении или запросе.

6.1.1.6. В случае если запрашиваемая субъектом информация, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно на Лицей или направить повторный запрос в целях получения запрашиваемой субъектом информации и ознакомления с такими персональными данными не ранее чем через тридцать дней (далее – нормированный срок запроса) после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.1.1.7. Субъект персональных данных вправе обратиться повторно в Лицей или направить повторный запрос в целях получения запрашиваемой субъектом информации, а также в целях ознакомления с обрабатываемыми персональными данными, до истечения нормированного срока запроса в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимой для запроса информацией должен содержать обоснование направления повторного запроса.

6.1.1.8. Лицей вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса возлагается на Лицей.

6.1.2. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных

6.1.2.1. Принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, Лицеем не осуществляется.

6.1.3. Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации

6.1.3.1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации, Лицеем не осуществляется.

6.1.4. Право на обжалование действий или бездействия Лицея

6.1.4.1. Если субъект персональных данных считает, что Лицей осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Лицея в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

6.1.4.2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

6.2. Обязанности Лицея

6.2.1. Обязанности Лицея при сборе персональных данных

6.2.1.1. При сборе персональных данных Лицей предоставляет субъекту персональных данных по его просьбе запрашиваемую информацию, касающуюся обработки его персональных данных в соответствии с частью 7 статьи 14 Федерального закона «О персональных данных».

6.2.1.2. Если в соответствии с федеральным законом предоставление персональных данных и (или) получение Лицеем согласия на обработку персональных данных являются обязательными, Лицей разъясняет субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.

6.2.1.3. Если персональные данные получены не от субъекта персональных данных, Лицей до начала обработки таких персональных данных предоставляет субъекту персональных данных следующую информацию (далее – информация, сообщаемая при получении персональных данных не от субъекта персональных данных):

- наименование и адрес Лицея или представителя Лицея;
- цель обработки персональных данных и ее правовое основание;
- перечень персональных данных;
- предполагаемые пользователи персональных данных;
- установленные Федеральным законом «О персональных данных» права субъекта персональных данных;
- источник получения персональных данных.

6.2.1.4. Лицей не предоставляет субъекту информацию, сообщаемую при получении персональных данных не от субъекта персональных данных, в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных Лицей;
- персональные данные получены Лицеем на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем
или поручителем, по которому является субъект персональных данных;
- обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона «О персональных данных»;
- предоставление субъекту персональных данных информации, сообщаемой при получении персональных данных не от субъекта персональных данных, нарушает права
и законные интересы третьих лиц.

6.2.1.5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Лицей обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации, обрабатываемых
в информационных системах с использованием баз данных, находящихся на территории Российской Федерации.

6.2.2. Меры, направленные на обеспечение выполнения Лицеем своих обязанностей

6.2.2.1. Лицей принимает меры, необходимые и достаточные для обеспечения выполнения своих обязанностей. Лицей самостоятельно определяет состав
и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, если иное не предусмотрено федеральными законами. К таким мерам, в частности, относятся:

- назначение ответственного за организацию обработки персональных данных;

– издание Политики, локальных нормативных актов по вопросам обработки персональных данных, а также локальных нормативных 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 Лицей не предусмотренные законодательством Российской Федерации полномочия и обязанности);

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

– осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям к защите персональных данных, Политике, локальным нормативным актам Лицея;

– оценка вреда, который может быть причинен субъектам персональных данных
в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых Обществом мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

– ознакомление работников Лицея, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями по защите персональных данных, документами, Политикой, локальными нормативными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

6.2.3. Меры по обеспечению безопасности персональных данных при их обработке

6.2.3.1. Лицей при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для 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.

6.2.3.2. Обеспечение безопасности персональных данных достигается, в частности:

– определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– учетом машинных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным
и принятием мер;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации

и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

6.2.4. Обязанности Лицея при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных

6.2.4.1. Лицей сообщает в установленном порядке субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней, в случае направления Лицея в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.2.4.2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Лицей дает в письменной форме мотивированный ответ в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней, в случае направления Лицеем в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.2.4.3. Лицей предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Лицей вносит в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Лицей уничтожает такие персональные данные. Лицей уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

6.2.4.4. Лицей сообщает 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 Лицея в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.2.5. Обязанности Лицея по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных

6.2.5.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных, Лицей осуществляет блокирование

неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Лицея) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, Лицей осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Лицея) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

6.2.5.2. В случае подтверждения факта неточности персональных данных Лицей на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Лицея) в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.2.5.3. В случае выявления неправомерной обработки персональных данных, осуществляемой Лицеем или лицом, действующим по поручению Лицея, Лицей в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению Лицея. В случае если обеспечить правомерность обработки персональных данных невозможно, Лицей в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Лицей уведомляет субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

6.2.5.4. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Лицей с момента выявления такого инцидента Лицеем, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомляет уполномоченный орган по защите прав субъектов персональных данных:

- 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, а также о лице, уполномоченном в Лицее для взаимодействия с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;
- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также о лицах, действия которых стали причиной выявленного инцидента (при наличии).

6.2.5.5. В случае достижения цели обработки персональных данных Лицей прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка

персональных данных осуществляется другим лицом, действующим по поручению Лицея) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Лицея) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Лицеем и субъектом персональных данных либо если Лицей не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

6.2.5.6. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Лицей прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Лицея) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Лицея) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Лицеем и субъектом персональных данных либо если Лицей не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

6.2.5.7. В случае обращения субъекта персональных данных с требованием о прекращении обработки персональных данных Лицей в срок, не превышающий десяти рабочих дней с даты получения соответствующего требования, прекращает их обработку или обеспечивает прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных, действующим по поручению Лицея), за исключением случаев, предусмотренных пунктами 2-11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона «О персональных данных». Указанный срок может быть продлен, но не более чем на пять рабочих дней, в случае направления Лицеем в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.2.5.8. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, Лицей блокирует такие персональные данные или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Лицея) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.2.6. Уведомление об обработке персональных данных

6.2.6.1. Лицей, за исключением случаев, предусмотренных Федеральным законом «О персональных данных», до начала обработки персональных данных уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

6.2.6.2. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление содержит следующие сведения:

- наименование, адрес Лицея;
- цель обработки персональных данных;
- описание мер, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных

данных, и номера их контактных телефонов, почтовые адреса и адреса корпоративной электронной почты;

– дата начала обработки персональных данных;

– срок или условие прекращения обработки персональных данных;

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

– сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;

– фамилия, имя, отчество физического лица или наименование юридического лица, имеющих доступ и (или) осуществляющих на основании договора обработку персональных данных, содержащихся в государственных и муниципальных информационных системах;

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

6.2.6.3. В случае изменения указанных сведений, а также в случае прекращения обработки персональных данных Лицей уведомляет об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

7. Сферы ответственности

7.1. Лица, ответственные за организацию обработки персональных данных в лицее

7.1.1. Лицей назначает лицо, ответственное за организацию обработки персональных данных.

7.1.2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от единоличного исполнительного органа Лицея, являющегося Оператором, и подотчетно ему.

7.1.3. Лицей предоставляет лицу, ответственному за организацию обработки персональных данных, необходимые сведения.

7.1.4. Лицо, ответственное за организацию обработки персональных данных, в частности, выполняет следующие функции:

– осуществляет внутренний контроль за соблюдением Лицеем и работниками Лицея законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– доводит до сведения работников Лицея положения законодательства Российской Федерации о персональных данных, локальных нормативных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– организовывает прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.

7.2. Ответственность

7.2.1. Лица, виновные в нарушении требований Федерального закона «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

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

8. Ключевые результаты

При достижении целей ожидаются следующие результаты:

обеспечение защиты прав и свобод субъектов персональных данных при обработке его персональных данных Лицеем;

повышение общего уровня информационной безопасности Лицея;

минимизация правовых рисков Лицея.

9. Связанные политики

Связанные политики отсутствуют.