ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ «ШКОЛА № 648 ИМЕНИ ГЕРОЯ РОССИЙСКОЙ ФЕДЕРАЦИИ А.Г. КАРЛОВА» (ГБОУ ШКОЛА № 648)

Флотская ул., д. 11, Москва, 125581
Телефон/факс: (495)-453-01-75, 8-495-454-24-91
ОКПО 33657057, ОГРН 1027700535422, ИНН 7712013764
E-mail: 648@edu.mos.ru

«Утверждаю»
Директор ГБОУ Школа № 648
Н.В. Горбатых _____
«31» августа 2020 г.

Правила осуществления внутреннего контроля соответствия персональных данных законодательству Российской Федерации в Государственном бюджетном общеобразовательном учреждении города Москвы «Школа № 648 имени Героя Российской Федерации А.Г. Карлова»

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия персональных данных законодательству Российской Федерации (далее – Правила) в Государственном бюджетном общеобразовательном учреждении города Москвы «Школа № 648 имени Героя Российской Федерации А.Г. Карлова» (далее – образовательная организация) определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным действующим законодательством, в том числе Федеральным законом от 27.07.2006 г. N 152-ФЗ «О персональных данных».

1.2. Правила разработаны с учетом требований Федерального закона от 27.07.2006 г. N 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 21.03.2011 N 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», иных нормативных правовых актов.

2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства

2.1. Цель проведения внутреннего контроля состоит в проверке и оценке соответствия обеспечения безопасности персональных данных (далее - ПДн) требованиям действующего законодательства, в том числе Федерального закона

от 27.07.2006 N 152-ФЗ «О персональных данных», деятельности образовательной организации в отношении обработки ПДн.

2.2. При проведении контроля используются процедуры документальной проверки, опрос и интервью с работниками образовательной организации. При необходимости уточнения результатов документальной проверки, опросов и интервью в рамках внутреннего контроля в качестве дополнительного способа может применяться «проверка на месте», которая проводится для обеспечения уверенности в том, что конкретные защитные меры реализуются, правильно используются и проверяются с помощью тестирования.

2.3. При проведении внутреннего контроля должно быть обеспечено документальное и, если это необходимо, техническое подтверждение того, что:

- деятельность образовательной организации в отношении обработки ПДн соответствует требованиям законодательства Российской Федерации;
- организационная структура обеспечения безопасности ПДн создана;
- процессы выполнения требований безопасности ПДн исполняются и удовлетворяют поставленным целям;
- защитные меры (межсетевые экраны, средства защиты информации от несанкционированного доступа и т.п.) настроены и используются правильно;
- остаточные риски безопасности ПДн оценены и остаются приемлемыми;
- рекомендации предшествующих проверок реализованы.

2.4. При проведении внутреннего контроля могут использоваться журналы средств защиты информации для выявления попыток несанкционированного доступа к защищаемым ресурсам, а также журнал учета нештатных ситуаций информационных систем персональных данных (далее - ИСПДн), ведущийся старшим лаборантом по электронным базам.

3. План внутренних проверок режима защиты персональных данных

N п/п	Мероприятие	Периодичность	Исполнитель
1.	Контроль за соблюдением режима защиты персональных данных, политики в отношении обработки персональных данных, за выполнением работниками обязанностей по защите персональных данных, определенных в организационно-распорядительной документации	Ежедневно	Старшим лаборант по электронным базам
2.	Контроль выполнения требований по режиму доступа в защищаемые помещения и на автоматизированные рабочие места, на которых производится обработка персональных данных	Ежедневно	Заместитель директора по управлению ресурсами
	Контроль соблюдения правил работы с носителями персональных данных	Ежедневно	Системный администратор

3.			
4.	Контроль целостности средств вычислительной техники, используемых для обработки персональных данных. Контроль корректной работы системного и прикладного программного обеспечения, средств защиты информации. Контроль состава технических средств.	Ежедневно	Системный администратор
5.	Контроль за соблюдением режима обработки персональных данных	Еженедельно	Старшим лаборант по электронным базам
6.	Пересмотр и, при необходимости, корректировка учетных записей пользователей	Еженедельно	Ответственный за АСИОУ Старшим лаборант по электронным базам
7.	Контроль за выполнением антивирусной защиты, неизменностью настроек средств антивирусной защиты и своевременным обновлением антивирусных баз	Еженедельно	Системный администратор
8.	Проверка журналов средств защиты информации для своевременного обнаружения фактов несанкционированного доступа к персональным данным	Еженедельно	Старшим лаборант по электронным базам
9.	Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации	Ежемесячно	Старшим лаборант по электронным базам
10.	Контроль за обеспечением резервного копирования, проверка работоспособности резервных копий	Ежемесячно	Ответственный за АСИОУ Старшим лаборант по электронным базам
11.	Поддержание в актуальном состоянии организационно-распорядительных документов	Ежегодно	Заместитель директора по управлению ресурсами

12.	Пересмотр организационно-распорядительной документации, регламентирующей порядок обработки персональных данных и требования по защите персональных данных, с учетом проводимых мероприятий по контролю	Ежегодно По факту изменения целей, технологии или иного значимого аспекта информационной безопасности	Заместитель директора по управлению ресурсами
13.	Обучение и повышение осведомленности работников в области защиты ПДн	Ежегодно В случае изменения законодательной базы, внутренних нормативных актов в области защиты персональных данных не позднее одного месяца с момента изменений	Заместитель директора по управлению ресурсами
14.	Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных	Раз в три года	Заместитель директора по управлению ресурсами
15.	Контроль заведения и удаления учетных записей пользователей	Прием/увольнение работника	Ответственный за АСИОУ Старшим лаборант по электронным базам

4. Заключительные положения

4.1. Настоящее Положение является локальным нормативным актом образовательной организации, утверждается приказом директора образовательной организации.

4.2. Все изменения и дополнения, вносимые в данное Положение, оформляются в письменной форме в соответствии с законодательством Российской Федерации.

4.3. После принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.