Муниципальное бюджетное дошкольное образовательное учреждение "Детский сад общеразвивающего вида №27 "Аленький цветочек" муниципального образования городской округ Симферополь Республики Крым (МБДОУ №27 "Аленький цветочек" г. Симферополя)

ПРИКАЗ

«01» 09 2025 г. №129

Симферополь

О назначении ответственного за организацию обработки персональных данных и других ответственных лиц

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) и принятыми в соответствии с ним нормативными правовыми актами, -

ПРИКАЗЫВАЮ:

1. Утвердить:

1) Должностную инструкцию ответственного за организацию обработки персональных данных в Муниципальном бюджетном дошкольном образовательном учреждении "Детский сад общеразвивающего вида №27 "Аленький цветочек" муниципального образования городской округ Симферополь Республики Крым (приложение 1);

2) Функциональные обязанности администратора информационной безопасности Муниципального бюджетного дошкольного образовательного учреждения "Детский сад общеразвивающего вида №27 "Аленький цветочек" муниципального образования городской округ Симферополь Республики Крым (приложение 2);

3) Функциональные обязанности администратора информационных систем Муниципального бюджетного дошкольного образовательного учреждения "Детский сад общеразвивающего вида №27 "Аленький цветочек" муниципального образования городской округ Симферополь Республики Крым (приложение 3);

2. Назначить ответственным за организацию обработки персональных данных из числа работников Муниципального бюджетного дошкольного образовательного учреждения "Детский сад общеразвивающего вида №27 "Аленький цветочек" муниципального образования городской округ Симферополь Республики Крым делопроизводителя МБДОУ №27 "Аленький цветочек" г. Симферополя Тищенко Н.А.

3. Ответственному за организацию обработки персональных данных:

1) организовать сбор и хранение в личных делах работников обязательств работников Муниципального бюджетного дошкольного образовательного учреждения "Детский сад общеразвивающего вида №27 "Аленький цветочек" муниципального образования городской округ Симферополь Республики Крым (далее – учреждение), непосредственно осуществляющих обработку персональных данных, в случае расторжения с ними трудового договора прекратить обработку персональных данных, ставшие известные им в связи с исполнением должностных обязанностей;

2) организовать сбор и хранение в личных делах работников учреждения согласий на обработку персональных данных, иных субъектов персональных данных;

3) в случаях, когда предоставление персональных данных является обязательным в соответствии с федеральным законом и (или) постановлением Правительства Российской Федерации, организовать процедуру разъяснения субъекту персональных данных юридических последствий отказа предоставления своих персональных данных;

4) провести оценку возможного вреда, который может быть причинён субъектам персональных данных, в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых учреждением мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

5) организовать проведение первичного инструктажа и (или) обучение по вопросам обработки персональных данных со всеми работниками учреждения, непосредственно осуществляющими обработку персональных данных;

6) организовать проведение первичного инструктажа и (или) обучение по вопросам обработки персональных данных со всеми принимаемыми на работу работниками, в должностные инструкции которых будет входить обработка персональных данных;

7) организовать проведение внепланового инструктажа и (или) обучение по вопросам обработки персональных данных с работниками учреждения, непосредственно осуществляющими обработку персональных данных, при значительных изменениях законодательства Российской Федерации, регулирующего сферу взаимоотношений, возникающих при обработке персональных данных, в том числе требований к защите персональных данных, документов, определяющих политику учреждения в отношении обработки персональных данных, локальных актов. Решение о необходимости внепланового инструктажа принимает ответственный за организацию обработки персональных данных учреждения в каждом отдельном случае;

8) обеспечить контроль ведения и хранение журнала ознакомления и (или) обучения. Хранение журнала осуществлять в местах, исключающих доступ к журналу посторонних лиц. Хранить журнал в течение 5 лет после завершения ведения.

4. Назначить ответственным за обеспечение безопасности информационных систем (далее – Администратор информационной безопасности) из числа работников Муниципального бюджетного дошкольного образовательного учреждения "Детский сад общеразвивающего вида №27 "Аленький цветочек" муниципального образования городской округ Симферополь Республики Крым заместителя заведующего по хозяйственной работе МБДОУ №27 "Аленький цветочек" г. Симферополя ЯрошевскогоВ.А.

5. Назначить ответственным за техническое обслуживание информационных систем из числа работников Муниципального бюджетного дошкольного образовательного учреждения "Детский сад общеразвивающего вида №27 "Аленький цветочек" муниципального образования городской округ Симферополь Республики Крым заместителя заведующего по хозяйственной работе МБДОУ №27 "Аленький цветочек" г. Симферополя Ярошевского В.А.

6. Администратору информационной безопасности:

1) участвовать в проведении классификации и (или) установлении уровня защищённости информации, содержащиеся в информационных системах учреждения;

2) определить актуальные угрозы безопасности информации и разработать «Модель угроз безопасности информации в информационных системах», а также, в случае необходимости, её согласование с регуляторами в области информационной безопасности (в пределах их компетенций). В случае применения средств криптографической защиты информации в информационных системах, разработать совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определить на этой основе и с учётом типа актуальных угроз требуемый класс средств криптографической защиты информации («Модель нарушителя»);

3) организовать учёт машинных носителей информации;

4) организовать проведение инструктажей работников, работающих с защищаемой информацией в информационных системах (далее – Пользователи ИС), по темам: правила работы в информационных системах, защита информации в информационной системе, положения законодательства в сфере защиты информации, новые угрозы в сфере защиты информации. Повышение осведомленности всех работников учреждения в вопросах информационной безопасности;

5) организовать доступ Пользователей ИС к ресурсам информационных систем, в соответствии с утвержденным заведующим перечнем лиц, допущенных к работе с информационными системами. Блокировать учётные записи, вносить изменения в полномочия и добавлять новых Пользователей ИС;

6) оказывать помощь Пользователям ИС, в части применения средств защиты от несанкционированного доступа и других средств защиты, входящих в состав информационных систем;

7) участвовать в составе постоянно действующей комиссии по реагированию на инциденты информационной безопасности, расследованиях причин инцидентов безопасности и внесение по результатам таких расследований предложений по совершенствованию систем безопасности.

7. Назначить комиссию по установлению уровня защищённости персональных данных в информационных системах персональных данных в составе, согласно приложению 4 к настоящему приказу.

8. Комиссии по установлению уровня защищённости персональных данных в информационных системах персональных данных в своей работе руководствоваться требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные 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». В месячный срок, с даты подписания данного приказа, а также, при изменении состава и (или) условий обработки персональных данных в информационных система: комиссия предоставляет заведующему на утверждение по результатам работ акты об установлении уровня защищённости персональных данных в информационных системах персональных данных учреждения.

9. Для анализа инцидентов информационной безопасности, в том числе определения источников и причин возникновения инцидентов, а также оценки их последствий, планирования и принятия мер по предотвращению повторного возникновения инцидентов, назначить постоянно действующую комиссию по работе с инцидентами в составе, согласно приложению 5 к настоящему приказу.

10. Председателю комиссии по работе с инцидентами информационной безопасности:

1) председателю и постоянно действующей комиссии по работе с инцидентами в своей работе руководствоваться «Положением по работе с инцидентами информационной безопасности» учреждения;

2) при необходимости привлекать к работе с комиссией работнико: учреждения, а также определять необходимость и выступать с инициативой о привлечении третьих лиц, не являющихся работниками учреждения, к работе с данной комиссией;

3) регистрировать в соответствующем журнале все инциденты информационной безопасности. Допускается ведение журнала в электронном виде;

4) обеспечить хранение журнала в местах, исключающих к нему доступ посторонних лиц. Хранить журнал в течение 5 лет после завершения ведения.

11. Назначить комиссию по уничтожению персональных данных субъектов персональных данных, согласно приложению 6 к настоящему приказу.

Комиссии по уничтожению персональных данных субъектов персональных данных руководствоваться требованиями, указанными в приложении 1 к настоящему приказу и утверждённым приказом Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций № 179 от 28 октября 2022 г. «Об утверждении Требований к подтверждению уничтожения персональных данных».

12. Контроль за выполнением настоящего приказа оставляю за собой.

13. Приказ вступает в силу со дня его подписания.

Заведующий Ю.Б. Веремьёва