АДМИНИСТРАЦИЯ
ПОСЕЛЕНИЯ РОГОВСКОЕ В ГОРОДЕ МОСКВЕ

РАСПОРЯЖЕНИЕ

От 11.01.2017 г. № 1

О вводе в действие
организационно-распорядительных документов

В целях реализации Федерального закона от 27.08.2006 N 152-ФЗ «О персональных данных»,

1. Принять в действие следующие документы:

– Должностная инструкция Специалиста — ответственного за организацию обработки персональных данных (Приложение 1);

– Положение о повышении осведомлённости работников в области обеспечения безопасности персональных данных (Приложение 2);

– Политика обработки персональных данных (Приложение 3);

– Правила обработки персональных данных (Приложение 4);

– Правила рассмотрения запросов субъектов персональных данных или их представителей по вопросам обработки их персональных данных (Приложение 5);

– Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение 6);

– Правила защиты информации при использовании сети Интернет (Приложение 7);

– Правила защиты информации при работе с электронной почтой (Приложение 8);

– Правила защиты информации средствами антивирусной защиты (Приложение 9);

– Правила защиты информации средствами парольной защиты (Приложение 10);

– Правила чистого стола и чистого экрана (Приложение 11);

– Инструкция о порядке обращения с машинными носителями персональных данных (Приложение 12);

– Инструкция по обработке персональных данных без использования средств автоматизации (Приложение 13);

– Инструкция пользователя информационной системы персональных данных (Приложение 14);

– Порядок доступа работников в помещения, в которых ведётся обработка персональных данных (Приложение 15);

– Перечень информационных систем персональных данных (Приложение 16);

– Перечень мест хранения материальных носителей персональных данных (Приложение 17);

– Перечень работников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (Приложение 18);

– Типовое обязательство работника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (Приложение 19);

– Типовая форма согласия на обработку персональных данных (Приложение 20);

– Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (Приложение 21);

2. Организовать размещение «Политики обработки персональных данных» на сайте администрации поселения Роговское в информационно – телекоммуникационной сети «Интернет» в течение 10 дней после её утверждения.
3. Ознакомить всех сотрудников, работающих с персональными данными под подпись.
4. Контроль исполнения настоящего Распоряжения оставить за главой администрации.

Глава администрации
поселения Роговское И.М. Подкаминский

Приложение 1
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ СПЕЦИАЛИСТА — ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1 Настоящая Должностная инструкция определяет обязанности, права и ответственность Специалиста — ответственного за организацию обработки персональных данных (далее — специалист) администрации поселения Роговское (далее — администрация).

1.2 Специалист назначается и освобождается от должности главой администрации.

1.3 Специалист получает указания непосредственно от главы администрации и подотчетен ему.

2. Должностные обязанности

Строго в рамках Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" специалист обязан:

2.1 Осуществлять внутренний контроль (надзор) за соблюдением администрацией и её работниками действующего законодательства РФ о персональных данных (далее — ПДн), в том числе требований к защите ПДн.

2.2 Доводить до сведения работников администрации положения действующего законодательства РФ о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн.

2.3 Осуществлять контроль за приёмом и обработкой обращений и запросов субъектов ПДн или их представителей по вопросам обработки их ПДн (перечень ПДн).

3. Права

Специалист при проведении контрольно-надзорных мероприятий вправе в пределах своей компетенции:

3.1 Использовать технику и оборудование, принадлежащую администрации.

3.2 Получать доступ к информационным системам ПДн в режиме просмотра и выборки необходимой информации.

3.3 Осуществлять мониторинг событий, связанных с безопасностью персональных данных.

3.4 Запрашивать и получать необходимые документы (сведения) для достижения целей проведения внутреннего контроля (надзора), в частности:

а) цели обработки ПДн;

б) категории ПДн;

в) категории субъектов, ПДн которых обрабатываются;

г) правовые основания обработки ПДн;

д) перечень действий с ПДн, общее описание используемых администрацией способов обработки ПДн;

е) описание мер, предусмотренных статьями 18.1 и 19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

ж) дата начала обработки ПДн;

з) сроки или условия прекращения обработки ПДн;

и) сведения о наличии или об отсутствии трансграничной передачи ПДн в процессе их обработки;

к) сведения о месте нахождения баз данных информации, содержащей ПДн граждан РФ;

л) сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите ПДн, установленными Правительством РФ.

3.5 Привлекать работников администрации при проведении контрольно-надзорных мероприятий, а также для анализа полученных материалов.

3.6 Расследовать события, связанные с нарушениями требований законодательства РФ в области ПДн и в случае необходимости выходить с предложениями по применению санкций (Нарушения требований действующего законодательства РФ и нормативно-правовых документов, регламентирующих вопросы обработки и безопасности ПДн влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ в отношении лиц, нарушивших требования нормативно-правовых документов по обработке и безопасности ПДн.

3.7 Выходить с предложениями *(например подготовка Справки или Служебной записки по ситуации)* по приостановлению или прекращению обработки ПДн, осуществляемой с нарушениями требований законодательства РФ в области ПДн.

3.8 Требовать уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем ПДн.

3.9 Разрабатывать и вносить предложения по изменению политики обработки ПДн администрации.

3.10Вносить предложения по изменению или принятию новых нормативно-правовых документов по обработке и безопасности ПДн.

3.11Принимать решения по вопросам, находящимся в рамках своей компетенции.

4. Ответственность

Специалист несет ответственность за:

4.1 Невыполнение своих обязанностей, определенных положениями настоящей инструкции, правилами и положениями администрации.

4.2 Невыполнение распоряжений и поручений главы администрации.

4.3 Непринятие мер по пресечению выявленных нарушений правил техники безопасности, противопожарным и другим правилам, создающим угрозу деятельности администрации, её работникам.

4.4 Несоблюдение трудовой и исполнительской дисциплины.

4.5 Специалист несет административную, гражданскую и уголовную ответственность в соответствии с действующим законодательством РФ.

5. Взаимодействия

Специалист осуществляет взаимодействия:

5.1 С руководителями структурных подразделений администрации — по вопросам подготовки документов, организации исполнения документов, подготовки и предоставления руководству необходимых документов и информации.

5.2 Со Службой правового обеспечения — по правовым вопросам, в том числе по вопросам согласования проектов документов.

6. Заключительные положения

Настоящая Должностная инструкция, изменения и дополнения к тексту настоящей Должностной инструкции вступают в силу с момента утверждения главой администрации в установленном порядке.

ЛИСТ ОЗНАКОМЛЕНИЯ

С Должностной инструкцией Специалиста — ответственного за организацию обработки персональных данных ознакомлен(а), копию Должностной инструкции получил(а):

№№ пп	ФИО	Дата	Подпись
1	2	3	4

Приложение 2
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ПОЛОЖЕНИЕ
О ПОВЫШЕНИИ ОСВЕДОМЛЁННОСТИ РАБОТНИКОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Положение о повышении осведомленности работников в области обеспечения безопасности персональных данных (далее — Положение) администрации поселения Роговское (далее — администрация) разработано в соответствии с требованием национального стандарта ГОСТ Р ИСО/МЭК 27002 и «Политики обработки персональных данных».

1.2. Настоящее Положение определяет организацию прохождения работниками администрации обучения по защите персональных данных (далее — ПДн), цели и виды проводимых обучений.

1.3. Целями настоящего Положения являются:

– формирование и поддержание необходимого уровня квалификации работников администрации с учетом требований по защите ПДн;

– обеспечение высокого уровня безопасности информационных и автоматизированных систем администрации.

1.4. В процессе обучения по вопросам защиты ПДн решаются следующие задачи:

– выработка и соблюдение правил по защите ПДн;

– разработка и внедрение системы обучения, включающей выявление потребности в обучении, планирование и бюджетирование, организацию обучения;

– построение обучения в соответствии со спецификой процессов администрации;

– формирование стандартов обучения;

– включение передового опыта, знаний, эффективных методов организации труда в процессе обучения работников защите ПДн;

– мотивация работников к повышению безопасности и обеспечению надежности работы.

2. Виды обучения

2.1. По формам планирования обучение подразделяется на плановое и внеплановое.

2.2. Плановое — проводится по следующим программам обучения:

– вводный инструктаж — проводится при поступлении руководителя или работника в администрацию;

– первичный инструктаж на рабочем месте — проводится при выполнении работ, к которым предъявляются дополнительные (повышенные) требования к защите ПДн;

– повторное обучение — проводится для руководителей подразделений и работников, выполняющие работы, к которым предъявляются дополнительные (повышенные) требования к защите ПДн, проводится один раз в три года.

2.3. Внеплановое — проводится по производственной необходимости, а также по заявкам руководителей структурных подразделений администрации (Приложение 2).

– внеочередное обучение — проводится при изменении требований к защите ПДн, изменениях в технологических процессах или при нарушениях требований по защите ПДн;

– целевое обучение — проводится при выполнении разовых работ, не связанных с прямыми обязанностями работников.

2.4. По формам проведения обучение подразделяется на индивидуальные и корпоративные (групповые), внутренние и внешние:

– индивидуальное обучение — проводиться с руководителем или работником персонально;

– корпоративное (групповое) — организация групп или обучение одновременно нескольких работников одного подразделения;

– внешнее — проводится с привлечением внешних обучающих организаций.

3. Организация обучения

3.1. Обучению в порядке, установленном настоящим Положением, подлежат:

– руководители и работники структурных подразделений администрации непосредственно на рабочих местах, в помещении специалиста — ответственного за организацию обработки персональных данных;

– практиканты, временные работники или работники, привлекаемые для работы в администрации по договорам;

– работники, выполняющие работы, к которым предъявляются дополнительные (повышенные) требования к защите ПДн.

3.2. Своевременность обучения по защите ПДн работников администрации контролирует специалист — ответственный за организацию обработки персональных данных.

3.3. Обучение и инструктаж проводятся в рабочее время.

3.4. Руководители и работники, вновь поступившие в администрацию, проходят первичный инструктаж у специалиста — ответственного за организацию обработки персональных данных.

3.5. Обучение фиксируются в Журнале проведения обучения по вопросам защиты ПДн (Приложение 1).

3.6. Внешнее обучение по вопросам защиты ПДн руководителей и работников проводится по программам, разработанным и утвержденным учебными центрами, организациями, институтами, имеющими разрешение на проведение обучения в данной области.

4. Ответственность

Специалист — ответственный за организацию обработки персональных данных несет ответственность за своевременное обучение работников администрации и ведение журнала проведения обучения по вопросам защиты ПДн.

5. Заключительные положения

5.1. Настоящее Положение принимается и вводится в действие распоряжением главы администрации.

5.2. Плановая проверка актуальности Положения проводится ежегодно специалистом — службы правового обеспечения с целью определения необходимости его пересмотра для обеспечения соответствия предусмотренного комплекса мероприятий реальным условиям и актуальным требованиям к обработке и безопасности ПДн.

5.3. Внеочередной пересмотр Положения производится в случае изменения действующего законодательства Российской Федерации и нормативно-правовых документов иных органов исполнительной власти.

5.4. Изменения и дополнения к тексту настоящего Положения вступают в силу с момента утверждения распоряжением главы администрации в установленном порядке.

Приложение 1
к Положению о повышении осведомленности работников
в области обеспечения защиты информации

ЖУРНАЛ
проведения обучения по вопросам защиты персональных данных

Дата	Вид обучения	Обучен/проверен	Подпись	Обучающий/ проверяющий	Подпись

Виды обучения:

- Вводный инструктаж;
- Первичный инструктаж на рабочем месте;
- Повторный инструктаж;
- Внеочередной инструктаж;
- Целевой инструктаж;
- Индивидуальное обучение;
- Корпоративное (групповое) обучение;
- Внешнее обучение.

Приложение 2
к Положению о повышении осведомленности работников
в области обеспечения защиты информации

ЗАЯВКА
на проведение обучения
по вопросам защиты персональных данных

Подразделение	
Должность	
ФИО	
Номер кабинета	

Провести обучение по следующим темам:

Тема	Дата

Привлечь специалистов для обучения по следующим темам:

Тема	Дата

Провести обучение во внешних организациях по следующим темам:

Тема	Дата

Приложение 3
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ПОЛИТИКА
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. С целью обеспечения выполнения норм Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" администрация поселения Роговское (далее — администрация) считает важнейшей задачей обеспечение легитимности обработки и безопасности персональных данных субъектов во всех процессах администрации.

Для решения данной задачи в администрации реализуется соответствующий комплекс мер и средств контроля и управления, которые представлены политиками, правилами, процессами, процедурами, а также функциями программных и аппаратных средств.

2. Настоящая Политика действует в отношении всех персональных данных, обрабатываемых администрацией в ходе своей деятельности.

3. Обработка персональных данных в администрации основана на следующих принципах:

− законность и добросовестность целей и способов обработки персональных данных;

− соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям;

− соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

− достоверность персональных данных, их актуальность и достаточность для целей обработки, недопустимость обработки избыточных по отношению к целям сбора персональных данных;

− легитимность организационных и технических мер по обеспечению безопасности персональных данных;

− непрерывность повышения уровня знаний работников администрации в сфере обеспечения безопасности персональных данных при их обработке;

− стремление к постоянному совершенствованию процессов обработки и безопасности персональных данных.

4. В администрации осуществляется обработка только тех персональных данных, которые представлены в утвержденном перечне персональных данных, обрабатываемых в администрации.

5. Администрация проводит оценку вреда, который может быть причинен субъектам персональных данных и определяет угрозы безопасности персональных данных.

6. Администрация применяет необходимые и достаточные организационные и технические меры, включающие в себя использование средств защиты информации, обнаружение фактов несанкционированного доступа, восстановление персональных данных, установление правил доступа к персональным данным, а также контроль и оценку эффективности применяемых мер.

7. Руководство администрации осознает необходимость и заинтересовано в обеспечении должного с точки зрения требований нормативных документов РФ уровня безопасности персональных данных, обрабатываемых в рамках выполнения основной деятельности.

8. В администрации назначено лицо, ответственное за организацию обработки персональных данных и определен порядок взаимодействия с субъектами по вопросам обработки их персональных данных. В случае возникновения вопросов, связанных с обработкой персональных данных администрацией, запрос ответственному лицу может быть направлен по адресу электронной почты: rogovskoe@yandex.ru

Приложение 4
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №01

ПРАВИЛА
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Термины и определения

1.1. **Информация** — сведения о чём-либо, независимо от формы их представления.

1.2. **Персональные данные** (далее — ПДн) — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

1.3. **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.

1.4. **Автоматизированная обработка ПДн** — обработка ПДн с помощью средств вычислительной техники.

1.5. **Использование ПДн** — действия (операции) с ПДн, совершаемые Администрацией в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц.

1.6. **Распространение ПДн** — действия, направленные на раскрытие ПДн неопределенному кругу лиц.

1.7. **Предоставление ПДн** — действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

1.8. **Блокирование ПДн** — временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

1.9. **Уничтожение ПДн** — действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

1.10. **Обезличивание ПДн** — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

1.11. **Несанкционированный доступ** (далее — НСД) — доступ к информации в нарушение должностных полномочий работника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации. Также НСД в отдельных случаях называют получение доступа к информации лицом, имеющим право на доступ к этой информации в объёме, превышающем необходимый для выполнения служебных обязанностей.

1.12. **Информационная система ПДн** (далее — ИСПДн) — совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

2. Общие положения

2.1. Правила обработки персональных данных (далее — Правила) устанавливают общие процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере ПДн, а также определяющие для каждой цели обработки ПДн содержание обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

2.2. Правила разработаны на основе анализа требований действующего законодательства

и нормативно-правовых документов, регламентирующих вопросы обработки и безопасности ПДн.

2.3. Настоящие правила защищают:

- ПДн;
- ИСПДн, обрабатывающие ПДн;
- ПДн, обрабатываемые в ИСПДн;
- информационные технологические процессы.

3. Основные цели и задачи обеспечения безопасности персональных данных

3.1. Основной целью обеспечения безопасности ПДн является минимизация ущерба (как непосредственного, так и опосредованного), возникающего вследствие возможной реализации угроз безопасности ПДн.

3.2. **Непосредственный ущерб** связан с причинением физического, материального, финансового или морального вреда субъекту ПДн и может проявляться в виде:

- нанесения вреда здоровью субъекта ПДн;
- незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта ПДн;
- потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием ПДн;
- нарушения конституционных прав субъекта ПДн вследствие вмешательства в его личную жизнь.

3.3. **Опосредованный ущерб** связан с причинением вреда обществу и (или) государству вследствие нарушения нормальной деятельности государственных органов, органов местного самоуправления, муниципальных органов, организаций различных форм собственности за счет неправомерных действий с ПДн.

3.4. Основной задачей обеспечения безопасности ПДн при их обработке в администрации является предотвращение НСД к ним, утечки по техническим каналам, предупреждение преднамеренных программно-технических воздействий с целью их разрушения (уничтожения) или искажения в процессе обработки, передачи и хранения ПДн.

4. Общие процедуры обеспечения безопасности персональных данных

4.1. Процедуры обеспечения безопасности ПДн разделяются на:

- административно-правовые;
- организационно-технические;
- экономические.

По времени применения процедуры обеспечения безопасности ПДн разделяются на:

- превентивные;
- восстановительные.

4.2. **Административно-правовые процедуры**

К административно-правовым процедурам защиты относятся нормы действующего законодательства и внутренние организационно-распорядительные документы администрации, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе обработки и использования ПДн, а также устанавливающие ответственность за нарушения этих правил, препятствуя неправомерному использованию ПДн и являющиеся сдерживающим фактором для реализации угроз безопасности потенциальными нарушителями.

4.3. **Организационно-технические процедуры**

Организационно-технические процедуры защиты основаны на использовании организационных мер, различных программных, аппаратных и программно-аппаратных средств, входящих в состав ИСПДн и выполняющих функции защиты информации, направленных на решение следующих задач:

– учет всех подлежащих защите ресурсов (ПДн, сервисов, каналов связи, серверов, автоматизированных рабочих мест и т.д.);

– своевременного обнаружения фактов НСД к ПДн;

– предотвращение НСД к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

– недопущения воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

– возможности восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;

– контроля за обеспечением уровня защищенности ПДн.

4.4. **Экономические процедуры**

Экономические процедуры обеспечения безопасности ПДн включают в себя:

– разработку программ обеспечения безопасности ПДн и определение порядка их финансирования;

– разработку мер поощрения и наложения штрафных санкций за соблюдение или не соблюдение установленных правил и процедур обработки ПДн.

4.5. **Превентивные процедуры**

Превентивные процедуры противодействия угрозам безопасности ПДн осуществляются на основе эффективного применения в процессе эксплуатации ИСПДн комплекса организационных, технических и технологических мероприятий, а также процедур и средств обеспечения функциональной устойчивости и безопасности работы ИСПДн.

Организационные мероприятия по обеспечению безопасности ПДн являются мероприятиями общего характера по организации деятельности работников, эксплуатирующих ИСПДн, порядку применения информационных технологий в помещениях, систематическому применению мер по недопущению вывода ИСПДн из строя.

Технические мероприятия по обеспечению безопасности ПДн заключаются в обслуживании, поддержании и управлении требуемым составом технических средств, обеспечивающих обработку ПДн в защищенном режиме.

Технологические мероприятия по обеспечению безопасности ПДн направлены на правильную реализацию функций и заданных алгоритмов работы ИСПДн, технологий обработки ПДн и защиту программ и ПДн от преднамеренных и непреднамеренных нарушений.

4.6. **Восстановительные процедуры**

Планирование восстановительных процедур определяется документом, устанавливающим требования к обязательным мероприятиям, проводимым заблаговременно и после возникновения нарушений, угрожающих штатному функционированию ИСПДн.

5. Обязанности и ответственность работников, допущенных к обработке персональных данных

5.1. Обработка ПДн осуществляется работниками, которые представлены в утверждённом «Перечне работников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным».

5.2. Работники, допущенные к обработке ПДн, обязаны:

– обрабатывать ПДн только в рамках выполнения своих должностных обязанностей;

– не разглашать ПДн полученные в результате выполнения своих должностных обязанностей, а также ставшие им известными по роду своей деятельности;

– пресекать действия других лиц, которые могут привести к разглашению (уничтожению, искажению) ПДн;

– при выявлении фактов разглашения (уничтожения, искажения) ПДн немедленно информировать руководителя структурного подразделения и специалиста — ответственного за организацию обработки ПДн;

– знать и выполнять требования настоящих Правил и нормативно-правовых документов, регламентирующих вопросы обработки и безопасности ПДн.

5.3. Обязанности работников, допущенных к обработке ПДн, регламентируются внутренними нормативно-правовыми документами, устанавливающими правила обращения со служебной информацией в администрации.

5.4. Нарушение работниками администрации требований действующего законодательства РФ и нормативно-правовых документов, регламентирующих вопросы обработки и безопасности ПДн влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

6. Содержание и категории обрабатываемых персональных данных

6.1. В администрации осуществляется обработка только тех ПДн, которые представлены в утвержденном «Перечне персональных данных».

6.2. Содержание и категории ПДн, обрабатываемых администрацией, определяются и соответствуют целям и правовым основаниями обработки ПДн.

7. Цели и правовые основания обработки персональных данных

7.1. Целями обработки ПДн является:

- рассмотрения резюме и подбора кандидатов на вакантные должности для дальнейшего трудоустройства;
- заключения, сопровождения, изменения, расторжения трудовых договоров, которые являются основанием для возникновения или прекращения трудовых отношений между работниками и работодателем;
- исполнения работодателем обязательств, предусмотренных федеральным законодательством, локальными нормативными актами и трудовыми договорами;
- содействия работникам в обучении и карьерном росте;
- содействия работникам в получении социальных льгот;
- сопровождения деятельности депутатов и руководителей администрации;
- подготовки финансовой отчетности администрации;
- заключения, сопровождения, изменения, расторжения договоров администрации;
- исполнения обязательств, предусмотренных договорами администрации;
- обработки и регистрации сведений, необходимых для реализации полномочий органа местного самоуправления;
- подготовки и направления ответов и разъяснений по заявлениям (обращениям), запросам физических и юридических лиц;
- взаимодействия с правоохранительными органами, а также с иными государственными органами по вопросам, входящим в их компетенцию.

7.2. Администрация осуществляет обработку ПДн в рамках реализации своих прав и законных интересов в соответствии с Уставом и требованиями, предусмотренными действующим законодательством РФ, в частности:

- Конституция РФ;
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Гражданский кодекс РФ;
- Трудовой кодекс РФ;
- Налоговый кодекс РФ;
- Федеральный закон от 15.12.2001 г. № 167-ФЗ «Об обязательном пенсионном страховании»;
- Постановление Правительства РФ от 27.11.2006 г. №719 «Об утверждении Положения о воинском учете»;
- Постановление Государственного комитета РФ по статистике от 05.01.2004 г. №1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;
- Федеральный закон от 21.07.1996 г. № 129-ФЗ «О бухгалтерском учете»;
- Федеральный закон от 27.07.2010 г. № 208-ФЗ «О консолидированной финансовой отчетности»;
- Федеральный закон от 02.05.2006 г. N 59-ФЗ "О порядке рассмотрения обращений граждан РФ";

– Федеральный закон от 06.10.2003 №131 ФЗ «Об общих принципах организации местного самоуправления в РФ»;
– Закон города Москвы от 22.10.2008 г. № 50 «О муниципальной службе в городе Москве»;
– Указ Президента РФ от 30 мая 2005 г. N 609 "Об утверждении Положения о персональных данных государственного гражданского служащего РФ и ведении его личного дела";
– Устав сельского поселения Роговское Подольского муниципального района Московской области от 13.04.2006 г. (принят решением совета депутатов сельского поселения Роговское Подольского муниципального района Московской области №8/4 от 13.04.2006 г.);
– иных нормативно-правовых документов.

8. Способы, сроки обработки и порядок уничтожения персональных данных

8.1. В администрации используется смешанная обработка ПДн.
8.2. Совокупность операций обработки ПДн включает:
– сбор;
– запись;
– систематизацию;
– хранение;
– уточнение;
– извлечение;
– использование;
– передачу (предоставление, доступ);
– блокирование;
– уничтожение.
8.3. Сроки обработки ПДн определяются из целей обработки ПДн в соответствии с требованиями нормативно-правовых документов, а также сроком исковой давности.
8.4. По достижению целей обработки или в случае утраты необходимости в достижении этих целей, обрабатываемые ПДн уничтожаются и составляется Акт об уничтожении, постоянно действующей экспертной комиссии администрации.
8.5. Уничтожение ПДн осуществляется в том числе:
– по требованию субъекта ПДн или уполномоченного органа по защите прав субъектов ПДн — если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
– при невозможности устранения администрацией допущенных нарушений при обработке ПДн;
– при отзыве субъектом ПДн согласия на обработку ПДн.
8.6. Принятие решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы на основании исключительно автоматизированной обработки ПДн, администрацией не производится.

9. Заключительные положения

9.1. Настоящие Правила принимаются и вводятся в действие распоряжением главы администрации.
9.2. Плановая проверка актуальности Правил проводится ежегодно Специалистом — ответственным за организацию обработки ПДн с целью определения необходимости их пересмотра для обеспечения соответствия предусмотренного комплекса мероприятий реальным условиям и актуальным требованиям к обработке и безопасности ПДн.
9.3. Внеочередной пересмотр Правил производится в случае изменения действующего законодательства РФ и нормативно-правовых документов иных органов исполнительной власти специалистом –службы правового обеспечения.
9.4. Изменения и дополнения к тексту настоящим Правилам вступают в силу с момента утверждения распоряжением главы администрации в установленном порядке.

Приложение 5
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ПРАВИЛА
РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ ПО ВОПРОСАМ ОБРАБОТКИ ИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1 Общие положения

1.1. Правила рассмотрения запросов субъектов персональных данных и их представителей по вопросам обработки их персональных данных (далее — Правила) администрации поселения Роговское (далее — администрация) разработаны в целях и рамках реализации Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

1.2. В пределах своей компетенции работники администрации принимают и обрабатывают обращения и запросы субъектов ПДн или их представителей по вопросам обработки их ПДн, указанных в «Перечне персональных данных».

1.3. Специалист — ответственный за организацию обработки ПДн (далее — Специалист) осуществляет контроль за приёмом и обработкой обращений и запросов субъектов ПДн или их представителей по вопросам обработки их ПДн.

1.4. Рассмотрение обращений и запросов субъектов ПДн или их представителей по вопросам обработки их ПДн осуществляется с учётом настоящих Правил и Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

2 Право и порядок доступа субъекта персональных данных к его персональным данным

2.1 В соответствии с действующим законодательством субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

а) факта обработки ПДн администрацией;

б) правовые основания и цели обработки ПДн;

в) цели и применяемые администрацией способы обработки ПДн;

г) наименование и место нахождения администрации, сведения о лицах (за исключением работников администрации), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с администрацией или на основании федерального закона;

д) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

е) сроки обработки ПДн, в том числе сроки их хранения;

ж) порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом «О персональных данных»;

з) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

и) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению администрации, если обработка поручена или будет поручена такому лицу;

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

2.2 Субъект ПДн вправе требовать от администрации уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав (образец требования приведён в *Приложении 1*).

2.3 Информация, указанная в пункте «2.1», предоставляются работником администрации субъекту ПДн в доступной форме, и в ней не должны содержатся ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

2.4 Информация, указанная в пункте «2.1», предоставляются субъекту ПДн или его представителю работником администрации при обращении либо при получении запроса субъекта ПДн или его представителя. Запрос должен содержать:

а) номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

б) сведения, подтверждающие участие субъекта ПДн в отношениях с Администрацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Администрацией, подпись субъекта ПДн или его представителя.

2.5 Запрос может быть направлен субъектом ПДн в форме электронного документа и подписан электронной подписью в соответствии с законодательством РФ (образец запроса приведён в *Приложении 2)*.

2.6 В случае, если информация, указанная в пункте «2.1», а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно к администрации или направить ему повторный запрос в целях получения информации, указанной в пункте «2.1», и ознакомления с такими ПДн не ранее чем через 30 (тридцать) дней 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 ПДн.

2.7 Субъект ПДн вправе обратиться повторно к администрации или направить повторный запрос в целях получения информации, указанной в пункте «2.1», а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в пункте «2.6», в случае, если такая информация и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте «2.4», должен содержать обоснование направления повторного запроса.

2.8 Работник вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами «2.6» и «2.7». Такой отказ мотивируется. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на работнике администрации.

2.9 Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе если:

а) обработка ПДн, включая ПДн, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

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

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

г) доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;

д) обработка ПДн осуществляется в случаях, предусмотренных законодательством РФ 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.

3 Право на обжалование действий или бездействия администрации поселения Роговское

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

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

4 Контроль и порядок учёта обращений и запросов по вопросам обработки ПДн

4.1 В целях осуществления контроля за приёмом и обработкой обращений и запросов субъектов ПДн или их представителей по вопросам обработки их ПДн Специалистом осуществляется их учёт.

4.2 Специалист открывает, ведет и хранит Журнал учета обращений по вопросам обработки персональных данных *(Приложение 3)*. Количество листов в журнале определяется из расчета срока использования от 3 до 5 лет.

4.3 Для достоверного и своевременного учёта обращений и запросов по вопросам обработки ПДн работники администрации обязаны предоставлять Специалисту следующую информацию:

а) сведения о лицах, запрашивающих информацию, указанную в пункте «2.1»;

б) краткое содержание обращений субъектов ПДн;

в) цели запросов субъектов ПДн;

г) сведения о предоставлении информации или об отказе в ее предоставлении;

д) дату передачи или отказа в предоставлении информации.

4.4 Информация предоставляется Специалисту в течении 5 (пяти) рабочих дней со дня передачи или отказа в предоставлении информации, указанной в пункте «4.1».

4.5 Специалист вносит полученную информацию в журнал, работники проверяют внесённую информацию и расписываются в нём.

4.6 Запрещается подчищать, стирать и изменять (исправлять) записи в журнале. В случае неправильных записей всю горизонтальную строку перечёркивают двумя чертами, скорректированные записи воспроизводятся в следующей (нижней) строке.

5 Заключительные положения

5.1. Настоящие Правила принимаются и вводятся в действие распоряжением главы администрации.

5.2. Плановая проверка актуальности Правил проводится ежегодно Специалистом с целью определения необходимости их пересмотра для обеспечения соответствия предусмотренного комплекса мероприятий реальным условиям и актуальным требованиям к обработке и безопасности ПДн.

5.3. Внеочередной пересмотр Правил производится в случае изменения действующего законодательства РФ и нормативно-правовых документов иных органов исполнительной власти.

5.4. Изменения и дополнения к тексту настоящим Правилам вступают в силу с момента утверждения распоряжением главы администрации в установленном порядке.

Приложения к настоящим Правилам:

Образец требования об уточнение персональных данных (Приложение 1)

Образец запрос на получение информации об обработки персональных данных (Приложение 2)

Журнал учёта обращений по вопросам обработки персональных данных (Приложение 3)

Все приложения являются неотъемлемой частью настоящих Правил.

Приложение 1
к Правилам рассмотрения запросов субъектов
персональных данных или их представителей

ОБРАЗЕЦ
ТРЕБОВАНИЯ ОБ УТОЧНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,

(Фамилия, имя, отчество полностью)

(вид документа, удостоверяющий личность) (серия) (номер) (выдан)

(кем и когда выдан)

(адрес регистрации)

(фактическое место проживания)

(реквизиты доверенности или иного документа, подтверждающего полномочия представителя субъекта персональных данных)

в соответствии с ч. 1, ст. 14 ФЗ от 27.07.2006 № 152-ФЗ требую внести изменения в мои персональные данные на основании сведений, содержащихся в следующих документах:

О результатах прошу сообщить по нижеуказанным контактам и адресу фактического места проживания.

(номер мобильного/сотового телефона) (адрес электронной почты)

(дата) (подпись)

Приложение 2
к Правилам рассмотрения запросов субъектов
персональных данных или их представителей

ОБРАЗЕЦ
ЗАПРОСА НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____
(Фамилия, имя, отчество полностью)

_____
(вид документа, удостоверяющий личность) (серия) (номер) (выдан)

_____
(кем и когда выдан)

_____
(адрес регистрации)

_____
(фактическое место проживания)

_____
(реквизиты доверенности или иного документа, подтверждающего полномочия представителя субъекта персональных данных)

в соответствии с ч. 1, ч. 4 ст. 14 ФЗ от 27.07.2006 № 152-ФЗ прошу предоставить мне следующую информацию:
1) подтверждение факта обработки персональных данных;
2) правовые основания и цели обработки персональных данных;
3) цели и применяемые способы обработки персональных данных;
4) наименование и место нахождения администрации, сведения о лицах (за исключением работников администрации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с администрацией или на основании федерального закона;
5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
6) сроки обработки персональных данных, в том числе сроки их хранения;
7) порядок осуществления субъектом персональных данных прав, предусмотренных ФЗ от 27.07.2006 № 152-ФЗ;
8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению администрации, если обработка поручена или будет поручена такому лицу.

О результатах прошу сообщить по нижеуказанным контактам и адресу фактического места проживания.

_____
(номер мобильного/сотового телефона) (адрес электронной почты)

_____
(дата) (подпись)

Приложение 3
к Правилам рассмотрения запросов субъектов
персональных данных или их представителей

ЖУРНАЛ
учета обращений по вопросам обработки персональных данных

Журнал начат «_____» _____ 20_____г. Журнал завершен «_____» _____20_____г.

_____ / Должность, ФИО /
_____ / Должность, ФИО /

Срок хранения завершенного журнала —3 года, считая с 01 января года, следующего за годом окончания ведения записей в журнале.
На 1 листе

№ п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи или отказа в предоставлении информации	Фамилия, имя, отчество. и подпись работника администрации
1						
2						
3						
4						
5						
6						

Приложение 6
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ПРАВИЛА
ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1 Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее — Правила) администрации поселения Роговское (далее — администрация) определяют сроки и последовательность действий Специалиста — ответственного за организацию обработки персональных данных (далее — специалист) либо комиссии, образуемой главой администрации поселения Роговское (далее — администрация).

1.2 В целях осуществления внутреннего контроля соответствия обработки персональных данных (далее — ПДн) установленным требованиям Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", администрация организует проведение периодических проверок условий обработки ПДн.

1.3 О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, главе администрации докладывает специалист либо председатель комиссии.

2. Предмет контроля (надзора)

Предметом внутреннего контроля (надзора) за соответствием обработки ПДн установленным требованиям являются проверка исполнения структурными подразделениями администрации:

- Порядка доступа работников в помещения, в которых ведётся обработка персональных данных;
- Инструкции о порядке обращения с машинными носителями персональных данных;
- Инструкции по обработке персональных данных без использования средств автоматизации;
- Инструкции пользователя информационной системы персональных данных;
- Правил защиты информации при использовании сети Интернет;
- Правил защиты информации при работе с электронной почтой;
- Правил защиты информации средствами антивирусной защитой;
- Правил защиты информации средствами парольной защиты;
- Правил обработки персональных данных;
- Правил чистого стола и чистого экрана.

3. Обязанности при осуществлении контроля (надзора)

Специалист либо комиссия при проведении проверки обязаны:

1) проводить проверку на основании распоряжения главы администрации;
2) соблюдать установленные сроки проведения проверки.

4. Описание результата исполнения функции внутреннего контроля (надзора)

Проверка завершается:

- составлением акта-проверки (*Приложение 1*);
- подготовкой и направлением материалов проверки главе администрации.

5. Срок исполнения функции внутреннего контроля (надзора)

Срок проведения не может превышать 20 (двадцать) рабочих дней.

6. Принятие решения о проведении проверки

6.1 Проверки проводятся на основании распоряжения главы администрации.

6.2 Решение о проведении проверки принимает глава администрации.

6.3 В день принятия решения специалист готовит проект распоряжения о проведении проверки и направляет его на подпись главе администрации.

6.4 В распоряжении о проведении проверки указываются:

– цели, задачи, предмет проверки;

– фамилии, имена, отчества должностных лиц, проводящих проверку;

– даты начала и окончания проведения проверки.

7. Проведение проверки

7.1 Проверка проводится специалистом либо комиссией, которые указаны в распоряжении о ее проведении.

7.2 Руководители, иные уполномоченные представители администрации должны обеспечить необходимые условия для проведения проверки и обязаны по требованию специалиста либо комиссии, проводящих проверку, организовать доступ к оборудованию, в помещения, где осуществляется обработка ПДн, предоставить необходимую информацию и документацию для достижения целей проверки.

7.3 В случае необоснованного препятствования проведению проверки, уклонения от участия в проведении проверки руководитель или иной уполномоченный представитель несут ответственность в соответствии с законодательством РФ.

7.4 В ходе проведения проверки специалист либо комиссия осуществляют мероприятия по контролю выполнения обязательных требований, установленных нормативно-правовыми документами администрации в области обработки и безопасности ПДн.

7.5 При проведении проверки специалист либо комиссия не вправе:

– требовать представления документов, информации, если они не относятся к предмету проверки;

– превышать установленные сроки проведения проверки.

8. Оформление результатов и принятие мер по результатам проверки

8.1 По результатам проверки специалистом составляется акт-проверки, который оформляется непосредственно после ее завершения.

8.2 По результатам проведения проверки специалистом либо комиссией, акт-проверки составляется в двух экземплярах. Один экземпляр акта с копиями приложений вручается руководителю или иному уполномоченному представителю под расписку об ознакомлении либо об отказе в ознакомлении с актом-проверки.

8.3 При наличии разногласий по содержанию акта-проверки окончательное решение принимает Специалист либо председатель комиссии, исполняющий функции руководителя проверки. Члены комиссии, а также руководитель или иной уполномоченный представитель, не согласные с принятым решением, вправе изложить в письменной форме свое особое мнение, которое прилагается к акту-проверки.

Акт подписывают специалист либо члены комиссии, проводившие проверку, после чего в него запрещается вносить изменения и дополнения.

К акту прилагаются справки, объяснительные работников администрации, на которых в соответствие с должностными инструкциями и нормативно-правовыми актами возложены обязанности по обработке и защите ПДн (Пояснение: Работники подписывают обязательства, в которых в п. 1 указано, что они обязаны соблюдать установленные «Политикой обработки персональных данных» принципы обработки персональных данных), меры, необходимые для устранения выявленных нарушений и другие документы, подтверждающие выявление (устранение) нарушения.

8.4 В случае выявления по результатам проверки нарушения требований законодательства РФ в области персональных данных в акте-проверки делаются записи об устранении выявленных нарушений.

8.5 По окончании проверки Специалист либо председатель комиссии в журнале учёта мероприятий по контролю соответствия обработки персональных данных установленным требованиям (*Приложение 2*) производит запись о проведенной проверке.

9. Заключительные положения

9.5. Настоящие Правила принимаются и вводятся в действие распоряжением главы администрации.

9.6. Плановая проверка актуальности Правил проводится ежегодно специалистом — ответственным за организацию обработки ПДн с целью определения необходимости их пересмотра для обеспечения соответствия предусмотренного комплекса мероприятий реальным условиям и актуальным требованиям к обработке и безопасности ПДн.

9.7. Внеочередной пересмотр Правил производится в случае изменения действующего законодательства РФ и нормативно-правовых документов иных органов исполнительной власти специалистом – службы правового обеспечения.

9.8. Изменения и дополнения к тексту настоящим Правилам вступают в силу с момента утверждения распоряжением главы администрации в установленном порядке.

Приложение 1
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

УТВЕРЖДАЮ
Глава администрации
поселения Роговское
_____ И.М. Подкаминский
«01» января 2016 г.

АКТ
от «01» января 2016 г. № 1
проверки соблюдения требований ФЗ от 27.07.2006 N 152-ФЗ "О персональных данных"

На основании распоряжения главы администрации поселения Роговское от _____ № _____ «О проведении проверки соблюдения требований ФЗ от 27.07.2006 N 152-ФЗ "О персональных данных" в период с 02.02.2000 по 20.02.2000 г. работниками администрации поселения Роговское в составе:

1)	ФИО специалиста или комиссии	должность
2)		
3)		

проведена проверка соблюдения требований ФЗ от 27.07.2006 N 152-ФЗ "О персональных данных".

1. Сведения о результатах проверки соблюдения требований ФЗ от 27.07.2006 N 152-ФЗ "О персональных данных" (констатация фактов соблюдения требований по вопросам проверки), в том числе о выявленных и устраненных в ходе проверки нарушениях, о лицах, на которых возлагается ответственность за совершение этих нарушений:

_____

_____

2. В ходе проверки выявлены следующие нарушения требований ФЗ от 27.07.2006 N 152-ФЗ "О персональных данных":

№ п/п	Конкретное описание (существо) выявленного нарушения	Наименование нормативного документа и номер его пункта, требования которого нарушены (не соблюдены)

На основании «Политики обработки персональных данных» предлагается устранить вышеуказанные нарушения.

3. К акту прилагаются документы, составленные при проверке, объяснения должностных лиц, работников, на которых возлагается ответственность за нарушения обязательных требований, другие документы или их копии, связанные с результатами мероприятия по контролю, меры, необходимые для устранения выявленных нарушений)

№ п/п	Наименование приложения

_____
(дата) (подпись)

_____
(дата) (подпись)

_____
(дата) (подпись)

Приложение 2
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

ФОРМА
журнала учёта мероприятий по контролю соответствия обработки персональных данных установленным требованиям

№ п/п	Наименование мероприятия	Краткое описание	Дата проведения мероприятия	Ф. И. О. лица, проводившего мероприятие	Подпись лица, проводившего мероприятие	Примечание

Приложение 7
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ПРАВИЛА
ЗАЩИТЫ ИНФОРМАЦИИ
ПРИ ИСПОЛЬЗОВАНИИ СЕТИ ИНТЕРНЕТ

1. Общие положения

1.1. Правила защиты информации при использовании сети Интернет (далее — Правила) администрации поселения Роговское (далее — Администрация) разработаны в соответствии с требованием национального стандарта ГОСТ Р ИСО/МЭК 27002 и «Политики обработки персональных данных».

1.2.Цели использования сети Интернет:

- получение и распространение информации, связанной с деятельностью администрации;
- обмен электронными сообщениями;
- информационно-аналитическая работа в интересах администрации;
- ведение дистанционного обслуживания населения.

1.3. Область действия настоящих Правил распространяется на всех работников администрации, допущенных к использованию сети Интернет.

2. Порядок использования сети Интернет

2.2. Доступ к сети Интернет предоставляется работникам администрации в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

2.3. Для доступа к сети Интернет применяется стандартное программное обеспечение операционных систем установленных на персональных компьютерах работников администрации.

3. Организация безопасности при использовании сети Интернет

3.1. Интернет не является защищенной средой и не обеспечивает конфиденциальности информации, передаваемой за пределы администрации.

3.2. Администрация оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством.

3.3. В администрации используются средства контроля, позволяющие протоколировать и анализировать данные о работе пользователей с ресурсами Интернет (посещаемые сервера, объем передаваемого трафика, время работы и т.д.). При необходимости, данная информация может быть предоставлена руководителям структурных подразделений, а также главе администрации для контроля.

3.4. Для ограничения использования сети Интернет в неустановленных целях в администрации организована система блокирования сервисов сети Интернет не соответствующих деятельности администрации.

3.5. Весь передаваемый входящий Интернет-трафик проходит проверку средствами антивирусной защиты в соответствии с документом «Правила защиты информации средствами антивирусной защиты».

4. Правила использования сети Интернет

При использовании сети Интернет запрещено:

- использовать предоставленный администрацией доступ в сеть Интернет в личных целях;
- использовать в служебной деятельности сервисы зарубежных информационно-телекоммуникационных сервисов (facebook, google, yahoo, dropbox, skype, whatsapp и др.), в частности: - онлайновые сервисы для планирования встреч, событий и дел с привязкой к календарю;

- веб-ориентированные приложения для работы с документами, допускающие совместное использование документов; - облачные хранилища; - электронные почтовые ящики; - сервисы обмена мгновенными сообщениями, видео- и голосовой связью;

– использовать специализированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к запрещенному контенту сети Интернет;

– публиковать, загружать и распространять материалы содержащие конфиденциальную информацию; информацию, полностью или частично, защищенную авторскими или другими правами, без разрешения владельца; вредоносное программное обеспечение; средства для несанкционированного доступа; идентификационные и аутентификационные данные (логины, пароли); серийные номера лицензионного программного обеспечения; угрожающую, клеветческую, непристойную информацию, а так же информацию, оскорбляющую честь и достоинство других лиц; материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и т.п.;

– фальсифицировать IP адрес своего персонального компьютера, а также прочую служебную информацию.

5. Ответственность

5.5. Работники администрации несут персональную ответственность за соблюдение данных Правил, а также за все действия, произведенные в сети Интернет с рабочего персонального компьютера.

5.6. При подозрении работника администрации в нецелевом использовании сети Интернет инициализируется служебная проверка.

5.7. По факту выясненных обстоятельств составляется акт расследования инцидента и передается непосредственному руководителю для принятия мер согласно нормативным актам администрации и действующему законодательству. Акт расследования инцидента и сведения о принятых мерах подлежат передаче специалисту — ответственному за организацию обработки персональных данных.

5.8. Ответственность системных администраторов:

– организация доступа к сети Интернет;

– администрирование, техническое обслуживание и настройка технических средств, при предоставлении или ограничении доступа к сети Интернет;

– участие в расследовании инцидентов защиты информации при использовании сети Интернет.

5.9. Ответственность специалиста — ответственного за организацию обработки персональных данных:

– разработка требований по обеспечению защиты информации при использовании сети Интернет;

– контроль исполнения настоящих Правил;

– анализ данных о работе работников в сети Интернет;

– расследование инцидентов защиты информации при использовании сети Интернет.

6. Заключительные положения

6.1. Настоящие Правила принимаются и вводятся в действие распоряжением главы администрации.

6.2. Плановая проверка актуальности Правил проводится ежегодно специалистом — ответственным за организацию обработки ПДн с целью определения необходимости их пересмотра для обеспечения соответствия предусмотренного комплекса мероприятий реальным условиям и актуальным требованиям к обработке и безопасности ПДн.

6.3. Внеочередной пересмотр Правил производится в случае изменения действующего законодательства Российской Федерации и нормативно-правовых документов иных органов исполнительной власти проводится специалистом – службы правового обеспечения.

6.4. Изменения и дополнения к тексту настоящим Правилам вступают в силу с момента утверждения распоряжением главы Администрации в установленном порядке.

Приложение 8
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ПРАВИЛА ЗАЩИТЫ ИНФОРМАЦИИ ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ

1. Общие положения

1.1. Правила защиты информации при работе с электронной почтой (далее — Правила) администрации поселения Роговское (далее — администрация) разработаны в соответствии с требованием национального стандарта ГОСТ Р ИСО/МЭК 27002 и «Политики обработки персональных данных».

1.2. Настоящие Правила определяют основные принципы и меры защиты информации при осуществлении работниками администрации электронного почтового обмена.

1.3. Объектами защиты Правил являются:

- входящие и исходящие сообщения электронной почты;
- архивы электронных почтовых сообщений.

2.Раскрытие электронной почты

2.1. Электронная почта является собственностью администрации, в частности:

- rogovskoe@yandex.ru;
- rogovskoe.kadry@mail.ru;
- rogovobuh@mail.ru;
- rogovo_sd@mail.ru.

2.2. Администрация располагает возможностью и имеет право, в случае необходимости просматривать, копировать, удалять, раскрывать и передавать государственным органам (или иным организациям) любое электронное сообщение, созданное, посланное или полученное с помощью электронной почты работника.

3. Порядок использования электронной почты

3.1. Электронная почта используется для обмена в рамках общедоступных сетей служебной информацией в виде электронных сообщений и документов в электронном виде.

3.2. Для обеспечения функционирования электронной почты допускается применение как бесплатного, так и коммерческого программного обеспечения, согласованного с специалистом — ответственным за организацию обработки персональных данных.

3.3. Все электронные сообщения и документы в электронном виде, передаваемые посредством электронной почты подлежат обязательной проверке на отсутствие вредоносного программного обеспечения согласно «Правилам защиты информации средствами антивирусной защиты».

4. Правила использования электронной почты

Работники обязаны:

4.1. Соблюдать требования настоящих Правил.

4.2. Ежедневно, в рабочие дни, проверять электронную почту.

4.3. Использовать электронную почту исключительно для выполнения своих должностных обязанностей.

4.4. Обязательно использовать заголовок "тема" письма для короткого пояснения содержания сообщения.

4.5. Проверять имя адресата перед отправкой сообщения, а также проверять, что сообщение отправлено по правильному адресу.

4.6. Удалять электронные сообщения, необходимость в которых отсутствует.

4.7. Ставить в известность специалиста — ответственного за организацию обработки персональных данных о любых фактах нарушения настоящих Правил.

Работникам запрещено:

4.8. Отправлять электронные письма от имени других работников, если иное не определено их должностными обязанностями.

4.9. Использовать электронную почту для отправки сообщений, содержащих угрозы, клевету, способных нанести вред администрации, её репутации, унижающих людей по расовому или половому признаку, призывающих к свержению действующего государственного строя, материалы сексуального характера и т.п., а также нарушающих работу работников администрации.

4.10. Отправлять сообщения содержащие исполняемые файлы, если иное не вызвано служебной необходимостью.

4.11. Открывать вложения подозрительных электронных сообщений. К подозрительным электронным сообщениям можно отнести письма:

- от незнакомых отправителей;
- содержащие исполняемые файлы (расширения .exe, .com, .bat и т.п.);
- содержащие предложения "открыть", "нажать", "запустить", "посетить" и т.п.

4.12. Использовать адрес электронной почты для оформления подписки на периодическую рассылку материалов из сети Интернет, не связанных с исполнением должностных обязанностей.

4.13. Пересылать на адреса внешней электронной почты электронные сообщения без разрешения первоначального отправителя.

4.14. Устанавливать постоянную пересылку с адресов электронной почты администрации на внешние адреса электронной почты.

4.15. Предпринимать попытки несанкционированного доступа к электронным сообщениям работников администрации, нарушения механизмов безопасности, перехвата электронной почты.

4.16. Участвовать в рассылке рекламных сообщений, если иное не вызвано служебной необходимостью и не входит в должностные обязанности.

4.17. Неправомочное использование, воспроизводство, передача, и распространение программного обеспечения или других материалов, защищенных в соответствии с национальными или международными законами об авторском праве, торговыми марками, или иными интеллектуальными правами собственности.

5. Ответственность

5.1.Работники администрации несут персональную ответственность за соблюдение данных Правил, а также за все действия, произведенные с использованием их электронной почты.

5.2.При подозрении работника администрации в нецелевом использовании электронной почты инициализируется служебная проверка.

5.3.По факту выясненных обстоятельств составляется акт расследования инцидента и передается непосредственному руководителю для принятия мер согласно нормативным актам администрации и действующему законодательству. Акт расследования инцидента и сведения о принятых мерах подлежат передаче специалисту — ответственному за организацию обработки персональных данных.

6. Заключительные положения

6.1.Настоящие Правила принимаются и вводятся в действие распоряжением главы администрации.

6.2.Плановая проверка актуальности Правил проводится ежегодно специалистом — ответственным за организацию обработки ПДн с целью определения необходимости их пересмотра для обеспечения соответствия предусмотренного комплекса мероприятий реальным условиям и актуальным требованиям к обработке и безопасности ПДн.

6.3.Внеочередной пересмотр Правил производится в случае изменения действующего законодательства Российской Федерации и нормативно-правовых документов иных органов исполнительной власти специалистом – службы правового обеспечения.

6.4.Изменения и дополнения к тексту настоящим Правилам вступают в силу с момента утверждения распоряжением главы администрации в установленном порядке.

Приложение 9
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ПРАВИЛА ЗАЩИТЫ ИНФОРМАЦИИ СРЕДСТВАМИ АНТИВИРУСНОЙ ЗАЩИТЫ

1.Общие положения

1.1. Правила защиты информации средствами антивирусной защиты (далее — Правила) администрации поселения Роговское (далее — администрации) разработаны в соответствии с требованием национального стандарта ГОСТ Р ИСО/МЭК 27002 и «Политики обработки персональных данных».

1.2. Настоящие Правила определяют основные принципы организации антивирусной защиты информации и устанавливает ответственность руководителей и работников подразделений, эксплуатирующих и сопровождающих информационные системы администрации.

1.3. Целью мероприятий по антивирусной защите является предотвращение потерь электронных информационных активов администрации.

1.4. Задачами антивирусной защиты являются:

– определение состава и регламента запуска антивирусных диагностических средств, регламента их ревизии и обновления;

– проведение профилактических работ с применением антивирусных диагностических средств;

– непрерывное обеспечение защиты информации от воздействия вредоносных программ на всех этапах эксплуатации электронных информационных систем администрации.

1.5. Объектами антивирусной защиты в администрации являются:

– все сервера (если иное не предусмотрено технологическим процессом);

– персональные компьютеры пользователей (в том числе ноутбуки);

– трафик электронного почтового обмена;

– трафик сети Интернет;

– съемные носители информации.

2. Организация мероприятий по антивирусной защите

2.1. Куратором организации работ по антивирусной защите выступает глава администрации.

2.2. Состав требований к системе антивирусной защиты определяет специалист (организация) — ответственный(ая) за обслуживания ПК администрации.

2.3. Планирование и проведение мероприятий по антивирусной защите организуют системные администраторы.

2.4. К использованию в администрации допускаются только лицензионные антивирусные средства (сертифицированный ФСТЭК), централизованно закупленные у разработчиков (поставщиков) указанных средств, рекомендованные к применению специалистом — ответственным за организацию обработки персональных данных.

2.5. В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение согласовывается с специалистом — ответственным за организацию обработки персональных данных.

2.6. В администрации организована постоянная антивирусная защита информационных систем в автоматическом режиме (если иное не предусмотрено технологическим процессом).

2.7. Установка средств антивирусной защиты на компьютерах в администрации осуществляется системными администраторы.

2.8.Настройка параметров средств антивирусной защиты осуществляется системными администраторами в соответствии с руководствами по применению конкретных антивирусных средств.

2.9. Система антивирусной защиты, предусматривает использование средств антивирусной защиты различных производителей.

3. Реагирование на инциденты

В случае обнаружения вредоносных программ в информационных системах администрации:

– системными администраторами совместно со специалистом — ответственным за организацию обработки персональных данных определяется область распространения вируса;

– производится внеплановая проверка информационных систем антивирусными средствами;

– при необходимости выносится решение о приостановлении работы системы до полного устранения действия вредоносной программы.

4. Профилактика вирусов

В администрации проводятся профилактические работы по выявлению и предотвращению возникновения и распространения вредоносных программ. К таким работам относятся:

– ежедневная автоматическая проверка наличия вредоносных программ на персональных компьютерах и серверах администрации;

– проверка всех программных продуктов, устанавливаемых на персональных компьютерах и серверах администрации на наличие вредоносного программного обеспечения;

– создание резервных копий программных продуктов;

– выборочные, внеплановые проверки персональных компьютеров и серверов;

– ограничение доступа к персональным компьютерам и серверам посторонних лиц.

5. Ответственность

5.1. Системные администраторы несут ответственность за:

– установку, поддержку и своевременное обновление антивирусного программного обеспечения в информационных системах администрации;

– реагирование на инциденты, связанные с работой антивирусной защиты.

5.2. Специалист — ответственный за организацию обработки персональных данных несёт ответственность за:

– периодические проверки функционирования антивирусного программного обеспечения;

– анализ событий, связанных с антивирусной защитой.

5.3. Работники структурных подразделений администрации, допущенные к работе в информационных системах, несут ответственность за:

– самостоятельное отключение (блокирование) работы антивирусного программного обеспечения на персональных компьютерах;

– использование съемных носителей информации без предварительной проверки наличия на них вредоносных программ;

– случайный или умышленный запуск вредоносного программного обеспечения со съемных носителей информации или из сети Интернет.

Приложение 10
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ПРАВИЛА ЗАЩИТЫ ИНФОРМАЦИИ СРЕДСТВАМИ ПАРОЛЬНОЙ ЗАЩИТЫ

1. Общие положения

1.1. Правила защиты информации средствами парольной защиты (далее — Правила) администрации поселения Роговское (далее — администрация) разработаны в соответствии с требованием национального стандарта ГОСТ Р ИСО/МЭК 27002 и «Политики обработки персональных данных».

1.2. Настоящие Правила определяют основные принципы организации парольной защиты информации и устанавливает ответственность руководителей и работников администрации, эксплуатирующих и сопровождающих информационные системы.

1.3. Целью мероприятий по парольной защите является предотвращение несанкционированного доступа к информационным активам администрации.

1.4. Задачами Правил являются:

– определение единых правил создания, смены, уничтожения и блокирования паролей для доступа пользователей в информационные системы администрации;

– минимизация угроз, связанных с несанкционированным доступом к конфиденциальной информации.

1.5. Объектами парольной защиты в администрации являются:

– операционные системы на персональных компьютерах пользователей (в том числе на ноутбуках);

– операционные системы на всех серверах администрации;

– информационные системы персональных данных;

– системы электронного документооборота;

– электронная почта;

– базы данных.

2.Организация мероприятий по парольной защите

2.1. Куратором организации работ по парольной защите выступает глава администрации.

2.2. Состав требований к системе парольной защиты определяет Специалист — ответственный за организацию обработки персональных данных.

2.3. Планирование и проведение мероприятий по парольной защите организуют системные администраторы.

3. Требования по безопасности паролей

Системные пароли.

3.1. Логины, поставляемые с операционными системами и техническим оборудованием (Administrator, Admin, Root и т.п.) должны быть заблокированы либо стандартные пароли к ним должны быть изменены на криптостойкие.

3.2. Пароли администраторов информационных систем должны быть уникальны для каждого типа таких систем (операционные системы на рабочих станциях, операционные системы на серверах, СУБД, BIOS, сетевое оборудование, удаленное управление и пр.).

Пароли пользователя.

3.3. Требования при назначении пароля новым пользователям:

– длина пароля должна быть не менее 8 символов (если информационная система или приложение не позволяют установить пароль указанной длины, следует руководствоваться рекомендациями по безопасности для данных систем);

– рекомендуется, чтобы пароль не включал в себя легко угадываемые сочетания символов (имена, фамилии, номера автомобилей, номера телефона, даты рождения и т.д.), общепринятые

сокращения (USER, ADMIN и т.д.), легко угадываемые сочетания или последовательности символов (123, qwerty, password) и т.д.

– пароль должен представлять собой сочетание букв (как в верхнем, так и в нижнем регистрах), цифр и специальных символов (@#$%^&*);

– пароль не должен быть названием сезона, месяцем года, днем недели или датой;

– пароль не должен повторяться или быть похожим на пароли, которые уже использовались в прошлом.

3.4. Информационные системы автоматически проверяют пароль при его смене и запрещают установку паролей, которые не соответствует вышеуказанным требованиям.

3.5.Вне зависимости от наличия встроенной в информационную систему проверки, ответственность за соответствие пароля правилам несет пользователь.

4. Смена паролей

4.1. В информационных системах, где пользователям доступна функция смены паролей, они производят первоначальную смену пароля при первом входе в систему.

4.2. В информационных системах смена паролей должна производиться не реже одного раза в год.

4.3. Срок действия паролей администраторов информационных систем не превышает 90 дней.

4.4. Внеплановая смена пароля пользователя операционной системы персонального компьютера осуществляется в случае выявления факта компрометации пароля. Смена пароля пользователя должна производиться немедленно после выявления факта компрометации пароля.

4.5. Внеплановая смена пароля администратора информационной системы осуществляется в случае выявления факта компрометации пароля, а также в случае прекращения полномочий системного администратора (увольнение, переход на другую должность и прочие обстоятельства). Смена пароля администратора информационной системы производится немедленно после выявления факта компрометации пароля, или прекращения полномочий системного администратора.

5. Ответственность

Работники администрации несут персональную ответственность за соблюдение настоящих Правил, а также за все действия, произведенные с использованием их учетной записи и пароля, в том числе за разглашение паролей и предоставления другим работникам (или третьим лицам) доступа к своему компьютеру.

Приложение 11
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ПРАВИЛА
ЧИСТОГО СТОЛА И ЧИСТОГО ЭКРАНА

1. Общие положения

1.1 Правила чистого стола и чистого экрана (далее — Правила) администрации поселения Роговское (далее — Администрация) разработаны в соответствии с требованием национального стандарта ГОСТ Р ИСО/МЭК 27002 и «Политики обработки персональных данных».

1.2. Правила разработаны с целью:

– снижения риска несанкционированного доступа, потери и повреждения информации как во время рабочего дня, так и вне рабочего времени;

– развития корпоративной культуры в отношении безопасного и надлежащего обращения с чувствительной или критической информацией и ее носителями;

– создание положительного имиджа перед посетителями администрации.

1.3. Область действия настоящих Правил распространяется на всех работников администрации.

1.4. Объектами защиты настоящих правил являются:

– бумажные документы;

– сменные носители информации (оптические диски CD, DVD, BLU-RAY; флэш-диски и другие устройства для хранения информации);

– средства обработки информации (планшеты, ноутбуки, персональные компьютеры).

2. Обязанности работников

Работники обязаны:

1. Выполнять настоящие правила и помогать коллегам в устранении их нарушений.
2. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами.
3. Носители (бумажные или электронные), содержащие чувствительную или критическую информацию, когда они не используются, убирать и (или) запирать (лучше всего, в несгораемый сейф или шкаф), особенно, когда помещение пустует.
4. Компьютеры, когда их оставляют без присмотра, выключать или защищать посредством механизма блокировки экрана или клавиатуры, контролируемого паролем (используются сочетание клавиш «эмблема WINDOWS + L» или «CTRL + ALT + DELETE», затем блокировать).
5. Предотвращать несанкционированное использование фотокопировальных устройств и другой воспроизводящей техники (сканеров, цифровых фотоаппаратов).
6. Документы, содержащие чувствительную или критическую информацию, немедленно изымать из принтеров.
7. Уничтожать документацию, содержащую чувствительную или критическую информацию шредерами и никогда, и ни при каких обстоятельствах не выбрасывать ее в скомканном виде.

3. Ответственность работников

Нарушения требований настоящих Правил, действующего законодательства РФ и нормативно-правовых документов, регламентирующих вопросы обработки и безопасности ПДн влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

Приложение 12
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ИНСТРУКЦИЯ
О ПОРЯДКЕ ОБРАЩЕНИЯ
С МАШИННЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1 Инструкция о порядке обращения с машинными носителями персональных данных (далее — Инструкция) администрации поселения Роговское (далее — администрация) разработана в целях реализации Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

1.2 Настоящая Инструкция устанавливает порядок учёта, хранения и уничтожения машинных носителей персональных данных (далее — ПДн) в администрации.

2. Организация учёта машинных носителей персональных данных

2.1 Для обработки ПДн в администрации используются следующие машинные носители ПДн:

– накопители на жёстких магнитных дисках (HDD);
– оптические диски (CD, DVD, BLU-RAY);
– флэш-диски;
– другие устройства для хранения информации.

2.2 Все машинные носители ПДн подлежат обязательному учёту с присвоением им уникальных регистрационных (идентификационных) номеров.

2.3 Для организации учёта машинных носителей ПДн распоряжением главы администрации назначается ответственное лицо.

2.4 Необходимые данные регистрируемого машинного носителя ПДн заносятся в Журнал учёта машинных носителей информации (Приложение 1).

2.5 При регистрации машинного носителя ПДн, помимо заполнения граф Журнала учёта, на его основу любым доступным способом наносятся следующие реквизиты:

– учётный номер по Журналу учёта;
– подпись лица, ответственного за организацию учёта.

2.6 Пример фиксации учётных данных на машинных носителях ПДн приведён в Приложении 2.

2.7 При невозможности доступа к машинному носителю ПДн с целью нанесения на него учётных данных такая информация наносится на корпус технического средства, в котором установлен машинный носитель ПДн.

2.8 Машинные носители ПДн снимаются с учёта в случае уничтожения на них ПДн. Уничтожение производится с использованием программных, аппаратных или программно-аппаратных средств.

3. Порядок хранения машинных носителей персональных данных

3.1 Организацию соблюдения порядка обращения с машинными носителями ПДн в структурных подразделениях администрации, работники которых имеют доступ к ПДн, осуществляют их непосредственные руководители.

3.2 Для хранения машинных носителей ПДн используются специальные хранилища (металлические шкафы, сейфы и т.п.), исключающие возможность несанкционированного к ним доступа, подмены, хищения или уничтожения.

3.3 Хранение машинных носителей ПДн осуществляется в условиях, исключающих воздействие на них теплового, светового (ультрафиолетового) или ионизирующего излучений. Не допускается размещение мест хранения машинных носителей ПДн вблизи источников сильных электромагнитных полей и приборов отопления.

3.4 При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки устройств с элементами накопления и хранения ПДн. Отладочные и экспериментальные работы (опробование программ, формирование массивов информации и др.) проводятся с использованием информации, не содержащей ПДн, либо при условии их обезличивания.

3.5 В случае необходимости передачи машинных носителей ПДн сторонней организации, такая передача может быть осуществлена только при условии заключения Соглашения о конфиденциальности ПДн с этой организацией.

4. Обязанности работников при обращении с машинными носителями персональных данных

4.1 Работник, осуществляющий работу с машинными носителями ПДн, обязан:

– обеспечивать надёжное хранение машинных носителей ПДн;

– не передавать машинные носители ПДн лицам, которые не допущены к обработке ПДн;

– осуществлять передачу машинных носителей ПДн другим лицам с обязательной отметкой об этом в Журнале учёта машинных носителей ПДн;

– своевременно сообщать непосредственному руководителю структурного подразделения и специалисту — ответственному за организацию обработки персональных данных о ставших ему известными попытках посторонних лиц получить доступ к защищаемым ПДн;

– немедленно уведомлять непосредственного руководителя и Специалиста — ответственного за организацию обработки персональных данных, и принимать меры по предотвращению утечки ПДн при выявлении фактов утраты или недостачи ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений;

– сдать машинные носители ПДн в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с обработкой ПДн.

5. Порядок уничтожения машинных носителей персональных данных

5.1 Машинные носители ПДн подлежат уничтожению в следующих случаях:

– при достижении целей обработки ПДн, если иное не предусмотрено законодательством РФ;

– если они пришли в негодность или отслужили установленный срок.

5.2 Уничтожение машинных носителей ПДн производится рабочей группой, назначенной распоряжением главы администрации, с оформлением Акта об уничтожении ПДн (Приложение 3).

5.3 Уничтожение ПДн, размещённых на машинных носителях ПДн, производится путём физического уничтожения носителя или путём удаления ПДн без повреждения носителя для обеспечения возможности его последующего использования.

5.4 Уничтожение машинных носителей ПДн производится любым способом, исключающим возможность дальнейшего использования элемента носителя информации, содержащего информационные массивы данных (область записи данных). Рекомендации по уничтожению машинных носителей ПДн приведены в *Таблице 1*

Таблица 1

Тип машинного носителя ПДн	Способ уничтожения (последовательность действий)
Накопители на жёстких магнитных дисках (HDD)	1) демонтаж корпуса 2) извлечение магнитных дисков 3) физическое дробление (значительная деформация) магнитных дисков и интегральных микросхем накопителя
Оптические диски (CD, DVD, BLU-RAY)	Измельчение оптического диска любым доступным механическим способом (например, в уничтожителе бумаги при наличии в нём такой функциональной возможности)
Флэш-диски	1) демонтаж корпуса 2) физическое дробление интегральных микросхем

6. Контроль учёта носителей персональных данных

Лица, ответственные за машинные носители ПДн, обязаны проводить периодический контроль (сверку) их наличия.

Приложение 1
к Инструкции о порядке обращения с машинными носителями персональных данных

ЖУРНАЛ
учёта машинных носителей персональных данных

№ п/п	Учётный номер	Дата постановки на учёт	Тип (модель) машинного носителя	Серийный (заводской) номер	Отметка о выдаче		Отметка в обратном приёме		Отметка об уничтожении носителя (информации)
					Фамилия и инициалы	Дата, подпись	Фамилия и инициалы	Дата, подпись	
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									

Приложение 2
к Инструкции о порядке обращения с машинными носителями персональных данных

ОБРАЗЦЫ
фиксации учётных данных на машинных носителях персональных данных

Жёсткий магнитный диск (HDD)

Оптический диск

Флэш-диск

Приложение 3
к Инструкции о порядке обращения с машинными носителями персональных данных

УТВЕРЖДАЮ
глава администрации
поселения Роговское
_____И.М. Подкаминский
«_____» _____ 2017 г.

АКТ
об уничтожении машинных носителей персональных данных

Комиссия в составе:

	Ф.И.О.	Должность
Председатель		
Члены комиссии		

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации _____ информация, записанная на них в процессе эксплуатации, подлежит уничтожению:

№ п/п	Учётный номер	Тип (модель) машинного носителя	Серийный (заводской) номер	Примечание

Всего подлежит уничтожению носителей _____
(цифрами и прописью)

После утверждения акта, перечисленные носители сверены с записями в акте и на указанных носителях персональные данные уничтожены путем _____
(стирания на устройстве гарантированного уничтожения информации и т.п.)

После утверждения акта, перечисленные носители сверены с записями в акте и уничтожены путем _____
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Уничтоженные носители с книг и журналов учета списаны.

Председатель _____/ /
Члены комиссии _____/ / _____/ /

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

Приложение 13
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ИНСТРУКЦИЯ
ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

1. Термины и определения

Материальный носитель персональных данных (далее — материальный носитель) — зафиксированная на материальном носителе информация с реквизитами, позволяющими идентифицировать субъекта персональных данных. Материальными носителями, в частности, могут быть: бумажные документы, электронные документы (формата .txt, .rtf, .doc) и т.д. и т.п.

2. Общие положения

2.1 Инструкция по обработке персональных данных без использования средств автоматизации (далее — Инструкция) администрации поселения Роговское (далее — администрация) разработана в целях реализации Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

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

2.3 Обработка ПДн не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что ПДн содержаться в ИСПДн либо были извлечены из нее.

2.4 Обработка ПДн, осуществляемая без использования средств автоматизации, применяется с учетом требований настоящей Инструкции.

3. Порядок и правила обработки персональных данных без использования средств автоматизации

3.1 ПДн при обработке без использования средств автоматизации обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

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

3.3 Работники администрации или лица, осуществляющие обработку ПДн без использования средств автоматизации по договору с администрацией, информируются о факте обработки ими ПДн, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, а также локальными правовыми актами администрации.

3.4 При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (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 ПДн, осуществляемой без использования средств автоматизации, имя (наименование) и адрес администрации, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых администрацией способов обработки ПДн;

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

в) типовая форма составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

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

3.5 При ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн на территорию, на которой находится администрация, или в иных аналогичных целях,

соблюдаются следующие условия:

а) при необходимости ведения такого журнала (реестра, книги) администрацией разрабатывается акт, содержащий сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов ПДн, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки ПДн, а также сведения о порядке пропуска субъекта ПДн на территорию, на которой находится администрация, без подтверждения подлинности ПДн, сообщенных субъектом ПДн;

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

в) ПДн каждого субъекта ПДн заносятся в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПДн на территорию, на которой находится администрация.

3.6 При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, принимаются меры по обеспечению раздельной обработки ПДн, в частности:

а) при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

б) при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

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

3.8 Правила, предусмотренные пунктами 3.6 и 3.7, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе ПДн и информации, не являющейся ПДн.

3.9 Уточнение ПДн 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 ПДн.

4. Меры по обеспечению безопасности персональных данных при обработке без использования средств автоматизации

4.1 Обработка ПДн, осуществляемая без использования средств автоматизации, осуществляется таким образом, что в отношении каждой категории ПДн определено место хранения ПДн (материальных носителей) и установлен перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

4.2 Обеспечивается раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

4.3 При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ. Перечень мер, необходимый для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются администрацией.

Приложение 14
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1 Настоящая Инструкция пользователя информационной системы персональных данных (далее — Инструкция) определяет основные обязанности, права и ответственность пользователей информационной системы персональных данных (далее — ИСПДн).

1.2 ИСПДн администрации поселения Роговское (далее — администрация) разрешается использовать для обработки персональных данных (далее — ПДн) при соблюдении следующих условий:

а) право работы в ИСПДн предоставляется только тем работникам, которые прошли инструктаж и официально имеют право допуска к обработке ПДн в соответствие с «Перечнем работников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным»;

б) каждый пользователь ИСПДн, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и информационным ресурсам ИСПДн, несет персональную ответственность за свои действия.

2. Обязанности пользователя информационной системы персональных данных

2.1 Знать и соблюдать установленные требования по безопасности ПДн, учету, хранению и пересылке машинных носителей информации, а также организационно-распорядительных документов Администрации в области обработки и безопасности ПДн.

2.2 Знать и строго выполнять правила работы со средствами защиты информации, используемыми на персональных компьютерах в составе ИСПДн.

2.3 Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн.

2.4 Выполнять в ИСПДн только те процедуры, которые определены для него в Руководстве пользователя и прочей эксплуатационной документации ИСПДн.

2.5 Соблюдать установленный режим разграничения доступа к информационным ресурсам ИСПДн, получать у системного администратора пароль, надежно его запоминать и хранить в тайне.

2.6 Хранить в тайне информацию о системе защиты, установленной в ИСПДн.

2.7 Немедленно ставить в известность руководителя подразделения и Специалиста — ответственного за организацию обработки ПДн:

2.7.1 обо всех фактах и попытках несанкционированного доступа (далее —НСД) к обрабатываемой ИСПДн информации или об ее исчезновении (искажении);

2.7.2 о фактах, а также о других причинах или условиях возможной утечки или разглашения ПДн;

2.7.3 нарушений целостности пломб на аппаратных средствах персональных компьютеров ИСПДн или иных фактов совершения в его отсутствие попыток НСД к ИСПДн;

2.7.4 об обнаружении недокументированных свойств и ошибок в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

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

2.8 В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов персональных компьютеров 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 системного администратора.

2.9 Ставить в известность системного администратора при необходимости произвести следующие действия:

2.9.1 обновление программного обеспечения;

2.9.2 модернизация аппаратных средств или изменение конфигурации ИСПДн;

2.9.3 вскрытие системных блоков персональных компьютеров, входящих в состав ИСПДн;

2.9.4 резервное копирование информации.

3. Запрещенные действия пользователя информационной системы персональных данных

3.1 Пользователю ИСПДн запрещается:

3.1.1 накапливать ненужные для работы ПДн;

3.1.2 самовольно вносить какие-либо изменения в конфигурацию технических средств персональных компьютеров ИСПДн или устанавливать дополнительно любые аппаратные средства;

3.1.3 производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств ИСПДн;

3.1.4 производить какие-либо действия по установке, настройке, тиражированию или модификации системного, специального и/или прикладного программного обеспечения, изменять установленный алгоритм функционирования технических и программных средств на персональных компьютерах ИСПДн;

3.1.5 использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;

3.1.6 отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами и установленные на компьютерах ИСПДн;

3.1.7 умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

3.1.8 обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам ИСПДн;

3.1.9 работать на персональных компьютерах ИСПДн при обнаружении каких-либо неисправностей;

3.1.10 привлекать посторонних лиц для производства ремонта технических средств ИСПДн.

4. Правила обращения с носителями информации

4.1 Пользователь ИСПДН, перед началом обработки на персональных компьютерах файлов, хранящихся на съемных носителях информации, должен осуществить проверку файлов на наличие компьютерных вирусов с использованием штатного антивирусного программного обеспечения, установленного на персональных компьютерах ИСПДн.

4.2 Пользователь ИСПДн обязан использовать для обработки ПДн, только учтенные съемные накопители информации (флэш-диски, CD, DVD, BLU-RAY и другие устройства для хранения информации), имеющие соответствующую маркировку и зарегистрированные в установленном порядке в журнале учета машинных носителей ПДн.

4.3 Пользователю ИСПДн запрещается:

4.3.1 выполнять работы с документами, содержащими ПДн, на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без письменного разрешения руководителя структурного подразделения;

4.3.2 производить копирование дискет, отдельных файлов с учтенных носителей информации на неучтенные носители информации, в том числе для временного хранения;

4.3.3 хранить носители информации вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;

4.3.4 хранить на учтенных носителях информации программы и данные, не относящиеся к рабочей информации;

4.3.5 производить вынос персональных компьютеров, на которых проводилась обработка ПДн, за пределы территории здания с целью их ремонта, замены и т. п. без письменного согласования со Специалистом — ответственным за организацию обработки ПДн.

5. Технология обработки персональных данных

5.1 При первичном допуске к работе в ИСПДн пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных документов администрации по вопросам обработки ПДн, изучает инструкцию пользователя ИСПДн, получает персональный идентификатор и личный пароль у системного администратора.

5.2 После изучения организационно-распорядительных (регламентирующих) документов пользователь совместно с системным администратором включает персональный компьютер ИСПДн, визуально убеждается в его технической исправности и нормальном функционировании.

5.3 В процессе работы пользователь производит обработку ПДн в ИСПДн в соответствии с «Руководством пользователя», должностной инструкцией, установленными в администрации внутренними процедурами и регламентами.

5.4 Порядок работы на персональном компьютере:

5.4.1 включить персональный компьютер;

5.4.2 после запроса необходимо набрать свое имя и пароль на клавиатуре;

5.4.3 при отсутствии НСД произойдёт загрузка операционной системы и персональный компьютер готов к работе;

5.4.4 при нарушении или сбое системы защиты об этом будет сообщено и в этом случае необходимо прекратить работу и пригласить системного администратора.

5.5 Вывод ПДн из ИСПДн осуществляется следующим образом:

5.5.1 копированием ПДн на учтенные носители;

5.5.2 передачей ПДн по каналам связи с применением шифрования (архивированием данных с помощью программного обеспечения WinRAR, WiZip и т.д.);

5.5.3 печатью на принтере.

6. Ответственность пользователя информационной системы персональных данных

6.1 На пользователя ИСПДн возлагается персональная ответственность за сохранность ПДн, обрабатываемых им в ИСПДн.

6.2 Нарушения требований настоящей Инструкции, действующего законодательства РФ и нормативно-правовых документов, регламентирующих вопросы обработки и безопасности ПДн влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

Приложение 15
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ПОРЯДОК
ДОСТУПА РАБОТНИКОВ В ПОМЕЩЕНИЯ,
В КОТОРЫХ ВЕДЁТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНФОРМАЦИИ

1. Ответственность за защиту информации и безопасность персональных данных в защищаемых помещениях, правильность использования установленных в них технических средств, наличие и сохранность имущества, несут ответственные за режим безопасности в защищаемых помещениях, назначенные распоряжением главы администрации поселения Роговское непосредственно на каждое помещение.
2. Установка нового оборудования, мебели, и т.п. или замена их, а также ремонт помещений необходимо проводить только по согласованию с лицом, ответственным за режим безопасности непосредственного помещения.
3. Установка новых или замена старых технических средств и систем, все работы по обслуживанию технических средств связи и распределенных коммуникаций проводятся только под контролем должностного лица, ответственного за режим безопасности непосредственного помещения.
4. Уборка помещений и все регламентные работы проводятся под контролем должностных лиц, имеющих право самостоятельного доступа в помещения согласно «Перечню работников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным».
5. В рабочее время в защищаемых помещениях обязательно должно присутствовать должностное лицо, имеющее право самостоятельного доступа в защищаемые помещения, согласно «Перечню работников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным»». При отсутствии таковых лиц нахождение кого-либо в защищаемых помещениях запрещается и помещения требуется закрывать на ключ.
6. При проведении закрытых мероприятий необходимо:
   - закрывать дверь в непосредственное помещение;
   - исключать нахождение посторонних лиц во время проведения закрытых мероприятий в коридоре блока помещений на минимальном удалении трех метров от дверей помещения.
7. В нерабочее время помещение закрывается на ключ и опечатывается.
8. Повседневный контроль за выполнением требований по защите помещений осуществляют должностные лица, имеющие право самостоятельного доступа в защищаемые помещения согласно «Перечню работников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным».
9. Периодический контроль эффективности мер защиты помещений осуществляется должностными лицами, назначенными распоряжением главы администрации поселения Роговское, по принципу «каждый ответственен за своё помещение».

Приложение 16
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ПЕРЕЧЕНЬ
ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ИС «1С: Бухгалтерия»
2. ИС «1С: Зарплата и Кадры»

Приложение 17
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ПЕРЕЧЕНЬ
МЕСТ ХРАНЕНИЯ МАТЕРИАЛЬНЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

№ п/п	Категории персональных данных	Название отдела	Номер кабинета	Способ и (или) место хранения
1	- граждане РФ	Отдел организационной работы и социального развития	5	сейф, металлический шкаф
2	- граждане РФ	Сектор организационной работы (в Отделе организационной работы и социального развития)	5	сейф, металлический шкаф
3	- представители компаний-контрагентов; - контрагенты-физические лица; - граждане РФ	Отдел финансово- налоговой политики и управления имуществом	7	сейф, металлический шкаф
4	- граждане РФ	Отдел жилищно-коммунального хозяйства и благоустройства	9	сейф, металлический шкаф
5	- внештатные специалисты (по договорам гражданско-правового характера); - муниципальные служащие (по трудовым договорам) - представители компаний-контрагентов; контрагенты-физические лица	Контрактная служба	6	
6	- кандидаты на вакантные должности; - внештатные специалисты (по договорам гражданско-правового характера); - муниципальные служащие (по трудовым договорам)	Сектор управления делами и муниципальной кадровой службы	3	сейф, металлический шкаф
7	- внештатные специалисты (по договорам гражданско-правового характера); - муниципальные служащие (по трудовым договорам) - представители компаний-контрагентов; - контрагенты-физические лица; граждане РФ	Служба правового обеспечения	3	
8	- граждане РФ	Служба безопасности, гражданской обороны и чрезвычайных ситуаций	12	сейф, металлический шкаф

Приложение 18
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ПЕРЕЧЕНЬ
РАБОТНИКОВ, ЗАМЕЩЕНИЕ КОТОРЫХ ПРЕДУСМАТРИВАЕТ ОСУЩЕСТВЛЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЛИБО ОСУЩЕСТВЛЕНИЕ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫХ

Глава администрации
Заместители главы администрации поселения

Начальники отделов
Заместители начальников отделов
Заведующие секторами
Заведующие секторами в составе отдела
Консультанты
Главный специалисты
Ведущие специалисты
Специалисты 1 категории
Главные эксперты
Эксперты

Приложение 19
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО
работника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я, _____,
(Фамилия, имя, отчество полностью)

_____
(должность)

работая в администрации поселения Роговское обязуюсь:

1. Не разглашать, не раскрывать публично, а также соблюдать установленные «Политикой обработки персональных данных» принципы обработки персональных данных, которые мне будут доверены или станут известны по работе.

2. Выполнять относящиеся ко мне требования «Политики обработки персональных данных», правил, инструкций, распоряжений и других нормативных-правовых документов по соблюдению правил обработки персональных данных и обеспечению их конфиденциальности.

3. В случае попытки посторонних лиц получить от меня сведения, составляющие персональные данные субъекта, немедленно сообщить руководителю структурного подразделения и Специалисту — ответственному за организацию обработки персональных данных.

4. Об утрате или недостаче документов, или иных носителей, содержащих персональные данные субъектов (удостоверений, пропусков и т.п.); ключей от хранилищ, сейфов (металлических шкафов) и о других фактах, которые могут привести к разглашению персональных данных субъектов, а также о причинах и условиях возможной утечки сведений немедленно сообщить руководителю структурного подразделения и Специалисту — ответственному за организацию обработки персональных данных.

5. В случае моего увольнения прекратить обработку персональных данных и все носители, содержащие персональные данные субъектов (документы, копии документов, черновики, дискеты, диски, flash-накопители, фотографии, видеоматериалы и пр.), которые находились в моем распоряжении в связи с выполнением мною трудовых обязанностей во время работы в администрации поселения Роговское, передать руководителю структурного подразделения или другому служащему по указанию руководителя структурного подразделения.

Я ознакомлен(а) с «Политикой обработки персональных данных».

Мне известно, что нарушение мною обязанностей по обработке и защите персональных данных может повлечь дисциплинарную, гражданско-правовую, административную, уголовную и иную ответственность в соответствии с законодательством РФ.

_____ _____
(дата) (подпись)

Приложение 20
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ТИПОВАЯ ФОРМА
согласия работника администрации поселения Роговское
на обработку персональных данных

Я, _____
(Фамилия, имя, отчество полностью)

_____
(вид документа, удостоверяющий личность) (серия) (номер) (выдан)

_____
(кем и когда выдан)

_____
(адрес регистрации)

_____
(фактическое место проживания)

настоящим предоставляю администрации поселения Роговское (далее — Администрация) свое согласие на обработку моих персональных данных (далее — Согласие) всеми способами, указанными в настоящем Согласии, включая получение их от меня и/или от любых третьих лиц, с учётом требований действующего законодательства РФ, и подтверждаю, что, предоставляя такое Согласие, я действую своей волей и в своем интересе.

Согласие предоставляется мною в целях заключения и дальнейшего исполнения с Администрацией Трудового договора, и сопутствующих ему договоров, обеспечивающих надлежащее исполнение Трудового договора, принятия решений или совершения иных действий, порождающих юридические последствия в отношении меня или других лиц.

Настоящее Согласие распространяется на следующую информацию, включая, но не ограничиваясь: мои фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, фотографии и иную информацию, относящуюся к моей личности, доступную либо известную в любой конкретный момент времени Администрации в связи с заключением и исполнением вышеуказанных договоров и необходимую для исполнения последних.

Настоящее Согласие предоставляется на осуществление следующих действий в отношении моих персональных данных, включая, но не ограничиваясь: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение, а также осуществление иных необходимых действий с моими персональными данными с учётом действующего законодательства РФ.

Способы обработки персональных данных, на совершение которых дается Согласие, следующие: смешанная обработка персональных данных; с передачей по внутренней сети Администрации; с передачей по сети Интернет; без осуществления трансграничной передачи.

Настоящим я признаю и подтверждаю, что в случае необходимости предоставления персональных данных для достижения указанных выше целей третьему лицу (в том числе банковской организации), а равно как при привлечении третьих лиц к оказанию услуг в указанных целях, передаче Администрацией принадлежащих ей функций и полномочий иному лицу, Администрация вправе в необходимом объёме раскрывать для совершения вышеуказанных действий информацию обо мне лично (включая мои персональные данные) таким третьим лицам, их агентам и иным уполномоченным ими лицам, а также предоставлять таким лицам соответствующие документы, содержащие такую информацию.

Также настоящим признаю и подтверждаю, что настоящее Согласие считается данным мною любым третьим лицам, указанным выше, с учётом соответствующих изменений, и любые такие третьи лица имеют право на обработку персональных данных на основании настоящего Согласия.

Настоящее Согласие предоставляется на срок действия Трудового договора и сопутствующих договоров, и любых правоотношений, возникающих в связи с исполнением (неисполнением, ненадлежащим исполнением) Трудового договора.

Настоящее Согласие может быть отозвано в порядке направления соответствующего письменного отзыва в Администрации. В этом случае Администрация прекращает обработку персональных данных, а персональные данные подлежат уничтожению, если отсутствуют иные правовые основания для обработки, установленные законодательством РФ.

По вопросам, связанным с обработкой персональных данных, с Администрацией можно связаться по электронной почте rogovskoe@yandex.ru, либо по адресу: Российская Федерация, 142167, г. Москва, поселение Роговское, поселок Рогово, ул. Юбилейная, дом 1А.

(дата) (подпись)

Приложение 21
к распоряжению администрации
поселения Роговское
от 11.01.2017г. №1

ТИПОВАЯ ФОРМА РАЗЪЯСНЕНИЯ
субъекту персональных данных юридических последствий отказа предоставить персональные данные

Мне, _____
(Фамилия, имя, отчество полностью)

разъяснены юридические последствия отказа предоставить свои персональные данные уполномоченным лицам администрации поселения Роговское.

Я предупрежден(а), что в случае отказа предоставления своих персональных данных администрация не сможет осуществлять обработку персональных данных.

Мне известно, что администрация для осуществления и выполнения функций, полномочий и обязанностей в установленной сфере деятельности в соответствии с законодательством Российской Федерации вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2 — 11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

По вопросам, связанным с обработкой персональных данных, с администрацией можно связаться по электронной почте rogovskoe@yandex.ru, либо по адресу: Российская Федерация, 142167, г.Москва, поселение Роговское, поселок Рогово, ул. Юбилейная, дом 1А.

_____ _____
(дата) (подпись)