МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ГИМНАЗИЯ № 2»
(МБОУ «ГИМНАЗИЯ № 2»)
«2 №-а ГИМНАЗИЯ» МУНИЦИПАЛЬНӦЙ ВЕЛӦДАН СЬӦМКУД УЧРЕЖДЕНИЕ

УТВЕРЖДАЮ
Директор МБОУ «Гимназия № 2»
_____ Н.В. Яловая
приказ МБОУ «Гимназия № 2»
от 30.12.2015 № 459

СОГЛАСОВАНО
протокол заседания
общего собрания
от 27.12.2015 № 2

ПОЛОЖЕНИЕ
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение обработки персональных данных (далее — Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» персональных данных.

1.2. Цели разработки Положения:

1.2.1. определение принципов и порядка обработки персональных данных работников и клиентов/контрагентов в в Муниципальном бюджетном общеобразовательном учреждении «Гимназия № 2» (далее — Гимназия);

1.2.2. обеспечение защиты прав и свобод работников, клиентов/контрагентов Гимназии при обработке их персональных данных, а также установление ответственности лиц, обрабатывающих персональные данные, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения:

1.3.1. настоящее Положение вступает в силу с момента его утверждения приказом и действует бессрочно, до замены его новым Положением;

1.3.2. пересмотр требований Положения производится ответственным (лицом, комиссией) за организацию обработки персональных данных не реже одного раза в год;

1.3.3. все изменения в Положение вносятся приказом Гимназии.

1.4. Контроль соблюдения требований настоящего Положения и контроль принятых организационных и технических мер осуществляет ответственный за организацию обработки персональных данных, назначенный приказом по Гимназии.

1.5. Все работники Гимназии, имеющие доступ к персональным данным, должны быть ознакомлены с настоящим Положением под роспись, в соответствии с приказом о доступе.

2. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

В настоящем Положении используются следующие основные понятия и определения:

2.1. *персональные данные* − любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2.2. *оператор* − государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

2.3. *обработка персональных данных* − любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию,

накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

2.4. *автоматизированная обработка персональных данных* – обработка персональных данных с помощью средств вычислительной техники;

2.5. *распространение персональных данных* – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

2.6. *предоставление персональных данных* - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

2.7. *блокирование персональных данных* - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

2.8. *уничтожение персональных данных* - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

2.9. *обезличивание персональных данных* - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

2.10. *информационная система персональных данных* (далее - ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

2.11. *конфиденциальность персональных данных* - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их раскрытия третьим лицам и распространения без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

2.12. *документированная информация* - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

2.13. *средство защиты информации* – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации;

2.14. *информационные технологии* – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

2.15. *контролируемая зона* - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посетителей, а также транспортных, технических и иных материальных средств.

3. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Необходимость обработки персональных данных с использованием средств автоматизации, а также без использования таких средств обусловлена сложившейся практикой обработки документов, содержащих персональные данные и рядом нормативно-правовых актов Российской Федерации.

3.2. Обработка персональных данных в Гимназии осуществляется, руководствуясь следующими документами: Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; Трудовой кодекс РФ; Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан российской федерации»; Устав Гимназии.

4. ЦЕЛИ ОБРАБОТКИ, СОДЕРЖАНИЕ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Цели обработки персональных данных, содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований определяются Перечнем персональных данных и Политикой обработки персональных данных, утвержденными распорядительным актом Гимназии.

4.2. Категории персональных данных, которые субъект может сделать общедоступными, описывается Перечнем персональных данных и определяется в Согласии на обработку

персональных данных.

4.3. Пересмотр пунктов Перечня и Политики производится ответственным (лицом, комиссией) за организацию обработки персональных данных при изменении штатной структуры Гимназии, но не реже одного раза в год.

5. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (за исключением случаев, предусмотренных частью 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»), в том числе содержащей:

5.1.1. подтверждение факта обработки персональных данных оператором;

5.1.2. правовые основания и цели обработки персональных данных;

5.1.3. цели и применяемые оператором способы обработки персональных данных;

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

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

5.1.6. сроки обработки персональных данных, в том числе сроки их хранения;

5.1.7. порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

5.1.8. информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

5.1.10. иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

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

5.3. Эти сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Запрос должен содержать:

5.3.1. номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;

5.3.2. сведения о дате выдачи указанного документа и выдавшем его органе;

5.3.3. сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором;

5.3.4. подпись субъекта персональных данных или его представителя.

5.4. В случае, если указанные сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения указанных сведений и ознакомления с персональными данными не ранее чем через 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 является субъект персональных данных.

5.5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему

повторный запрос в целях получения указанных сведений, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока (тридцать дней) в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос дополнительно должен содержать обоснование направления повторного запроса.

5.6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 6.4 и 6.5 настоящего Положения. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

5.7. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5.8. Запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам регистрируются в журнале обращений (приложение 2). Данный журнал ведется в подразделениях, где осуществляется сбор персональных данных (отдел кадров, обособленные подразделения, филиалы и т.п.). Журнал хранится в течение пяти лет с момента внесения последней записи, после чего уничтожается ответственным (лицом, комиссией) за организацию обработки персональных данных.

5.9. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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

6. ОБЯЗАННОСТИ РАБОТОДАТЕЛЯ И РАБОТНИКОВ ГИМНАЗИИ, РАБОТАЮЩИХ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

6.1. Работники Гимназии, допущенные к персональным данным, несут ответственность за точное выполнение требований, предъявляемых к ним в целях обеспечения сохранности указанных сведений. До получения доступа к работе, связанной с обработкой персональных данных, им необходимо изучить настоящее Положение и дать письменное обязательство о сохранении персональных данных (конфиденциальной информации).

6.2. Работники Гимназии, допущенные к персональным данным должны:

6.2.1. не разглашать персональные данные. о ставших им известной утечке персональных данных сообщать непосредственному руководителю и ответственному за организацию обработки персональных данных;

6.2.2. знакомиться только с теми документами и выполнять только те работы, к которым они допущены;

6.2.3. соблюдать правила пользования документами, содержащими персональные данные. не допускать их необоснованной рассылки;

6.2.4. выполнять требования режима: исключающие возможность ознакомления с персональными данными посторонних лиц, включая и своих работников, не имеющих к указанным документам прямого отношения;

6.2.5. использовать информационные ресурсы гимназии только для достижения целей деятельности гимназии (не использовать в личных целях);

6.2.6. при ведении деловых переговоров с представителями сторонних организаций или частными лицами ограничиваться выдачей минимальной информации, действительно необходимой для их успешного завершения.

6.3. Обязанности работодателя (оператора):

6.3.1. операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6.3.2. оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами. К таким мерам могут, в частности, относиться:

6.3.3. назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

6.3.4. издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

6.3.5. применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

6.3.6. осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

6.3.7. оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

6.3.8. ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

6.3.9. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных (а при сборе персональных данных через интернет – также опубликовать документ в интернет).

6.3.10. Оператор обязан представить документы и локальные акты, указанные в пункте 6.3, и (или) иным образом подтвердить принятие мер, указанных в пункте 6.3.2, по запросу уполномоченного органа по защите прав субъектов персональных данных.

6.3.11. Предоставляет работнику необходимые условия для выполнения требований по охране конфиденциальных сведений, к которым допускается работник.

6.4. Работник разрешает Гимназии производить контроль использования им информационных ресурсов Гимназии, а также использования им технических средств обработки, хранения и

передачи информации, предоставленных Гимназией для выполнения работником договорных обязанностей.

6.5. Гимназия оставляет за собой право, но не принимает каких-либо обязательств контролировать использование работником информационных ресурсов, технических средств обработки, хранения и передачи информации, а также соблюдения мер по охране конфиденциальных сведений.

7. ПОРЯДОК СБОРА, ХРАНЕНИЯ, ИСПОЛЬЗОВАНИЯ И ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Сбор, обработка

7.1.1. Обработка персональных данных допускается в следующих случаях:

7.1.1.1. обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных (на обработку сведений о здоровье и биометрических данных дается письменное согласие);

7.1.1.2. обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

7.1.1.3. обработка персональных данных необходима для исполнения договора, стороной которого является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных;

7.1.1.4. обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7.1.1.5. обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7.1.1.6. обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

7.1.1.7. обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных;

7.1.1.8. осуществляется обработка персональных данных, сделанных общедоступными субъектом персональных данных;

7.1.1.9. осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

7.1.1.10. в иных случаях, описанных в ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

7.1.2. Сбор персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений, настоящим Положением и приказами Гимназии.

7.1.3. Все персональные данные работника Гимназии следует получать у него самого, либо его законных представителей. Должностное лицо Гимназии должно сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, куда могут передаваться персональные данные и последствиях отказа работника дать письменное согласие на их получение и обработку.

7.1.4. Если получение персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

7.1.5. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных пунктом 7.1.6 настоящего Положения, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных

следующую информацию:

7.1.5.1. наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

7.1.5.2. цель обработки персональных данных и ее правовое основание;

7.1.5.3. предполагаемые пользователи персональных данных;

7.1.5.4. установленные настоящим Федеральным законом права субъекта персональных данных;

7.1.5.5. источник получения персональных данных.

7.1.6. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные пунктом 7.1.5 настоящего Положения, в случаях, если:

7.1.6.1. субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

7.1.6.2. персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

7.1.6.3. персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

7.1.6.4. оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

7.1.6.5. предоставление субъекту персональных данных сведений, предусмотренных пунктом 7.1.5 настоящего Положения, нарушает права и законные интересы третьих лиц.

7.1.7. Гимназия не обрабатывает персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях. В соответствии со ст. 24 Конституции Российской Федерации оператор вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

7.1.8. Работник, законный представитель предоставляет работнику Гимназии развитию достоверные сведения о себе. Работник проверяет достоверность сведений, сверяя данные, предоставленные работником, с имеющимися документами.

7.1.9. Ввод персональных данных в автоматизированные ИСПДн Гимназии осуществляется работником в соответствии с его должностными обязанностями.

7.1.10. Работники, осуществляющие ввод и обработку данных с использованием автоматизированных ИСПДн Гимназии, несут ответственность за полноту введенной информации и не должны вносить изменения, противоречащие информации, полученной непосредственно от субъекта персональных данных.

7.2. Согласие на обработку персональных данных

7.2.1. В следующих случаях Гимназия получает от субъекта согласие на обработку его персональных данных:

7.2.1.1. поручение обработки персональных данных другому лицу;

7.2.1.2. раскрытие третьим лицам или распространение персональных данных, если иное не предусмотрено федеральным законом;

7.2.1.3. обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;

7.2.1.4. включение персональных данных субъекта в общедоступные источники персональных данных, в том числе публикация в средствах массовой информации и интернет (согласие в письменной форме);

7.2.1.5. обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни (согласие в письменной форме);

7.2.1.6. обработка сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность

(биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных (согласие в письменной форме);

7.2.1.7. трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных (согласие в письменной форме);

7.2.1.8. принятие решения на основании исключительно автоматизированной обработки персональных данных субъекта, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы (согласие в письменной форме).

7.2.2. Работник Гимназии, либо лицо, поступающее на работу в Гимназию, являясь субъектом персональных данных, своей волей и в своем интересе принимает решение о предоставлении своих персональных данных и дает письменное согласие на их обработку (приложение 1а). Согласие с работника берется с целью признания части его персональных данных общедоступными.

7.2.3. Клиенты/контрагенты (физические лица), персональные данные которых обрабатывает Гимназия без заключения с ними договора, должны дать согласие на обработку их персональных данных (приложение 1б).

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

7.2.5. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пункте 7.1 и Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных».

7.2.6. Отзыв согласия на обработку персональных данных происходит по письменному заявлению субъекта персональных данных на имя директора Гимназии с указанием причин отзыва. При подаче заявления необходимо предъявить основной документ удостоверяющий личность. После отзыва согласия все персональные данные, содержащиеся в ИСПДн с использованием средств автоматизации в течение десяти дней уничтожаются без возможности восстановления, о чем уведомляется субъект персональных данных, если иное не установлено законодательством Российской Федерации. Данные находящиеся на бумажных носителях передаются в архив и хранятся в течение сроков, установленных законодательством.

7.3. Передача персональных данных

7.3.1. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в

соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

7.3.2. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

7.3.3. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

7.3.4. При передаче персональных данных субъекта оператор (Гимназия) должен соблюдать следующие требования:

7.3.4.1. не сообщать персональные данные субъекта третьей стороне без согласия субъекта, за исключением случаев, предусмотренных пунктом 7.1.1 настоящего Положения, а также в случаях, установленных федеральным законодательством;

7.3.4.2. предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц исполнения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

7.3.4.3. разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции;

7.3.4.4. передавать персональные данные субъекта представителям субъектов в порядке, установленном Трудовым, Семейным кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций.

7.3.5. В соответствии с законодательством Российской Федерации персональные данные, обрабатываемые Гимназией, могут быть переданы правоохранительным, судебным органам, органам социальной защиты и другим учреждениям, которые имеют на это право на основании федерального законодательства, а также в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороноспособности страны и безопасности государства без получения согласия субъекта персональных данных.

7.3.6. Решение о передаче информации, содержащей персональные данные, обрабатываемые в Гимназии, третьим лицам, за исключением указанного в пункте 7.3.5 настоящего Положения, принимается директором (заместителем директора) Гимназии только на основании мотивированного письменного запроса, если иное не предусмотрено договором или федеральным законодательством. Мотивированный запрос должен быть подписан уполномоченным должностным лицом, содержать указание цели и правовое основание предоставления персональных данных, срок предоставления этой информации, если иное не установлено федеральными законами.

7.3.7. Порядок передачи информации, содержащей персональные данные, обрабатываемые Гимназией, внутри Гимназии определяется должностными обязанностями работников или приказами Гимназии, в соответствии с законодательством РФ.

7.4. Хранение и уничтожение

7.4.1. Персональные данные могут храниться в бумажном и(или) электронном виде в отделе кадров, бухгалтерии (других подразделениях Гимназии) с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации и локальными нормативными актами мер по защите персональных данных. Право на доступ к местам хранения персональных данных предоставляется работникам структурных подразделений и(или) должностным лицам, определенным настоящим Положением, а также приказами о доступе к персональным данным, распорядительными документами Гимназии.

7.4.2. Хранение персональных данных в ИСПДн осуществляется на серверах и автоматизированных рабочих местах Гимназии с использованием специализированного программного обеспечения.

7.4.3. Хранение персональных данных должно осуществляться в форме, позволяющей

определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является субъект персональных данных.

7.4.4. Обрабатываемые персональные данные подлежат уничтожению (либо обезличиванию) в следующих случаях:

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

7.4.4.2. по требованию субъекта персональных данных, его представителя или уполномоченного органа по защите прав субъектов персональных данных, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными, неправомерно обрабатываемыми или не являются необходимыми для заявленной цели обработки;

7.4.4.3. отзыв субъектом персональных данных согласия на обработку его персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

7.4.5. Уничтожению не подлежат персональные данные, для которых законодательством РФ предусмотрены иные сроки хранения.

7.4.6. Уничтожению (стиранию) может подвергаться только сама информация о субъекте персональных данных, хранящаяся на носителе, либо сам носитель персональных данных.

7.4.7. По всем фактам уничтожения персональных данных или носителей персональных данных составляется акт (приложение 3).

7.5. Общедоступные персональные данные

7.5.1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

7.5.2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

7.6. Правила работы с обезличенными данными

7.6.1. Для обезличенных персональных данных нет необходимости обеспечения их конфиденциальности.

7.6.2. Для того, чтобы распространять, предоставлять третьим лицам, публиковать, передавать по незащищенным каналам связи и т.п. обезличенные персональные данные необходимо (перед совершением этих действий) убедиться в правильности проведения процедуры обезличивания персональных данных. Процедура обезличивания считается проведенной успешно, если по обезличенным персональным данным становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. При этом необходимо обеспечить конфиденциальность той дополнительной информации, с помощью которой возможно определить принадлежность персональных данных конкретному субъекту персональных данных.

8. ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ ПРЕДСТАВИТЕЛЕЙ

Таблица 1. Взаимодействие с субъектом персональных данных

№	Событие	Действие	Основания для отказа, исключения
1	Запрос субъекта ПДн на получение информации, касающейся обработки его персональных данных	Предоставить субъекту ПДн информацию по форме (Приложение 4) либо мотивированный отказ со ссылкой на п. 8 ст. 14 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» в течение 30 дней со дня получения запроса	см. п. 8 ст. 14 ФЗ «О персональных данных»
2	Предоставление субъектом сведений, подтверждающих, что обрабатываемые персональные данные являются неполными, неточными или неактуальными	Немедленно блокировать или обеспечить блокирование персональных данных на период проверки. Внести необходимые изменения в персональные данные в течение 7 рабочих дней со дня получения сведений. Уведомить субъекта персональных данных о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы	
3	Предоставление субъектом сведений, подтверждающих, что обрабатываемые персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки	Немедленно блокировать или обеспечить блокирование персональных данных на период проверки. Уничтожить такие персональные данные в течение 7 рабочих дней со дня получения сведений с составлением акта (Приложение 3).Уведомить субъекта персональных данных о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы	
4	Запрос уполномоченного органа по защите прав субъектов персональных данных	Ответить на запрос в течение 10 дней со дня получения запроса	
5	Обращение, запрос субъекта персональных данных либо уполномоченного органа по защите прав субъектов персональных данных о выявлении неправомерной обработки персональных данных	Немедленно блокировать или обеспечить блокирование персональных данных на период проверки. В течение 3-х рабочих дней со дня выявления неправомерной обработки – обеспечить правомерность обработки. Уничтожить в течение 10 рабочих дней со дня выявления неправомерной обработки – если невозможно обеспечить правомерность обработки	
6	Получение персональных данных субъектов от третьих лиц	Уведомить субъекта об обработке его персональных данных либо убедиться, что третье лицо (на основании заключенного договора с этим лицом о получении персональных данных) получило согласие субъекта персональных данных на передачу его персональных данных	

9. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ СУБЪЕКТОВ

9.1. Доступ работников к персональным данным осуществляется в соответствии со списками, которые утверждаются приказом по Гимназии.

9.2. Ознакомление лиц с персональными данными субъектов должно осуществляться только по необходимости и в тех объемах, которые необходимы для выполнения возложенных на них функций.

10. ОРГАНИЗАЦИЯ УЧЕТА ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ПДН

10.1. Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учету. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

10.2. При постановке на учет носителя ПДн их маркировка производится на нерабочей поверхности, посредством нанесения записей механическим путем или красящим веществом, имеющим хорошую механическую стойкость.

10.3. Учет и выдачу съемных носителей персональных данных осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Работники Гимназии получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

10.4. Доступ к носителям ПДн разрешается лицам, допущенным к обработке ПДн, и только в те интервалы рабочего времени, которые отведены для решения указанной задачи в графике рабочего времени.

10.5. Работа с носителями ПДн производится на рабочих местах лиц, допущенных к обработке ПДн.

10.6. Персональные компьютеры, используемые для обработки ПДн, подлежат инвентарному учету. В этих случаях, для контроля доступа к аппаратной части компьютера, крышки, неиспользуемые порты ввода-вывода указанных компьютеров опечатываются ответственным за обеспечение безопасности ПДн с проставлением печати Гимназии и образцами подписей ответственного за организацию обработки ПДн и работника, допущенного к обработке ПДн на данном рабочем месте.

11. ОБРАБОТКА ПДН, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

11.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных.

11.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

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

11.4. При фиксации ПДн на 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 должен использоваться отдельный носитель.

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

11.6. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации

производится путем обновления или изменения данных на носителе, а если это не допускается техническими особенностями носителя, - путем фиксации на том же носителе сведений о вносимых в них изменениях либо путем изготовления нового носителя с уточненными ПДн.

11.7. Необходимо обеспечивать раздельное хранение ПДн (носителей), обработка которых осуществляется в различных целях.

11.8. При хранении носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

12. Использование типовых форм документов и журналов однократного пропуска.

12.1. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

12.1.1. типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Гимназии, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Гимназией способов обработки персональных данных;

12.1.2. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

12.1.3. типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

12.1.4. типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

12.2. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию Гимназии или в иных аналогичных целях, должны соблюдаться следующие условия:

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

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

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

13. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

13.1. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на

технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

13.2. Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

13.3. Лица, получившие доступ к персональным данным, обязаны не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

13.4. В случае, если Гимназия на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

13.5. Меры по обеспечению конфиденциальности персональных данных, принимаемые в Гимназии, должны включать, но не ограничиваясь этим, следующее:

13.5.1. определение перечня персональных данных и мест обработки таких данных;

13.5.2. ограничение доступа к персональным данным, их носителям, путем установления порядка обращения с этими данными и носителями, контроля за соблюдением такого порядка;

13.5.3. учет лиц, получивших доступ к персональным данным, и (или) лиц, которым такие данные были предоставлены или переданы;

13.5.4. регулирование отношений по использованию персональным данным, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

13.5.5. учет носителей (документов), содержащих персональные данные.

13.5.6. организационные меры безопасности:

13.5.6.1. инструктаж работников по правилам обеспечения безопасности обрабатываемых персональных данных;

13.5.6.2. учет и хранение съемных носителей информации и порядок их обращения, исключающие хищение, подмену и уничтожение;

13.5.6.3. мониторинг и реагирование на инциденты информационной безопасности, связанные с персональными данными, включая проведение внутренних проверок, разбирательств и составление заключений;

13.5.6.4. постоянный контроль за соблюдением требований по обеспечению безопасности персональных данных (реализуется путем внутренних аудитов);

13.5.7. меры физической безопасности:

13.5.7.1. ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации. Распорядительным актом по Гимназии устанавливается контролируемая зона Гимназии, вводятся в действие Список помещений с ограниченным доступом и Список лиц, имеющих право посещать помещения Гимназии с ограниченным доступом. Лица, не указанные в Списке, в том числе обеспечивающие техническое и бытовое обслуживание (уборку, ремонт оборудования и технических средств), при наличии необходимости могут посещать помещения с ограниченным доступом в сопровождении ответственных лиц;

13.5.7.2. размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

13.5.7.3. организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

13.5.8. технические меры безопасности:

13.5.8.1. разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

13.5.8.2. регистрация действий пользователей и обслуживающего персонала, контроль доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

13.5.8.3. резервирование технических средств, дублирование массивов и носителей информации;

13.5.8.4. использование защищенных каналов связи;

13.5.8.5. предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

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

14.1. Контроль выполнения работ по обеспечению безопасности персональных данных в Гимназии (далее – Контроль) осуществляется путем проведения периодических контрольных мероприятий (в рамках внутренних аудитов) и внутренних проверок по фактам произошедших инцидентов информационной безопасности.

14.2. В рамках проведения контрольных мероприятий выполняются:

14.2.1. проверка наличия и актуальности планов, регистрационных журналов, актов, договоров, отчетов, протоколов и других свидетельств выполнения мероприятий по обеспечению безопасности персональных данных;

14.2.2. проверка осведомленности и соблюдения персоналом требований к обеспечению безопасности персональных данных;

14.2.3. проверка соответствия перечня лиц, которым предоставлен доступ к персональным данным, и их полномочий по доступу к определенным категориям персональных данных фактическому состоянию;

14.2.4. проверка локальных актов, определяющих условия хранения материальных носителей, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ, перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер;

14.2.5. проверка документов, определяющих места хранения персональных данных, перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

14.2.6. проверка документов об информировании лиц, осуществляющих обработку персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

14.2.7. проверка получения и передачи персональных данных третьим лицам с согласия субъекта персональных данных либо с последующим уведомлением субъекта о факте обработки его персональных данных;

14.2.8. проверка наличия и исправности функционирования технических средств защиты информации, используемых для обеспечения безопасности персональных данных, в соответствии с требованиями эксплуатационной и технической документации;

14.2.9. инструментальная проверка соответствия настроек технических средств защиты информации требованиям к обеспечению безопасности персональных данных (при необходимости);

14.2.10. проверка соответствия моделей угроз для информационных систем персональных данных условиям функционирования данных систем;

14.2.11. проверка соответствия организационно-распорядительной документации по обеспечению безопасности персональным данных действующим требованиям законодательства РФ, руководящих документов ФСБ России, ФСТЭК России.

14.3. Все собранные в ходе проведения контрольных мероприятий свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально.

14.4. Контрольные мероприятия проводятся как периодически в соответствии с планом и программой аудита, так и внепланово по решению директора Гимназии и в случае возникновения инцидентов информационной безопасности.

14.5. Внутренние проверки в Гимназии в обязательном порядке проводятся в случае выявления следующих фактов:
14.5.1. нарушение конфиденциальности, целостности, доступности персональных данных;
14.5.2. халатность и несоблюдение требований к обеспечению безопасности персональных данных;
14.5.3. несоблюдение условий хранения носителей персональных данных;
14.5.4. использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.
14.6. Задачами внутренней проверки являются:
14.6.1. установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
14.6.2. установление лиц, непосредственно виновных в данном нарушении;
14.6.3. выявление причин и условий, способствовавших нарушению.

15. СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

15.1. Ежегодно ответственный за организацию обработки персональных данных направляет директору Гимназии отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности персональных данных, обрабатываемых в Гимназии, вместе с перечнем предложений по совершенствованию системы защиты персональных данных.
15.2. Необходимость реализации мероприятий по совершенствованию системы защиты персональных данных может быть обусловлена:
15.2.1. результатами проведенных аудитов и контрольных мероприятий;
15.2.2. изменениями федерального законодательства в области персональных данных;
15.2.3. изменениями структуры процессов обработки персональных данных в пенсионном фонде;
15.2.4. результатами анализа инцидентов информационной безопасности;
15.2.5. результатами мероприятий по контролю и надзору за обработкой персональных данных, проводимых уполномоченным органом;
15.2.6. жалоб и запросов субъектов персональных данных.
15.3. На основании решения, принятого директором Гимназии по результатам рассмотрения ежегодного отчета и предложений по совершенствованию системы защиты персональных данных, ответственный за организацию обработки персональных данных составляет план работ по обеспечению безопасности персональных данных, обрабатываемых в Гимназии, на следующий год.

16. ПОРЯДОК РЕЗЕРВИРОВАНИЯ И ВОССТАНОВЛЕНИЯ МАССИВОВ И НОСИТЕЛЕЙ ИНФОРМАЦИИ

16.1. Резервному копированию подлежит информация следующих основных категорий:
16.1.1. обрабатываемые ПДн – не реже одного раза в неделю;
16.1.2. технологическая информация – не реже одного раза в месяц;
16.1.3. рабочие копии установочных компонент программного обеспечения — не реже одного раза в месяц;
16.1.4. эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – единожды и каждый раз при внесении изменений в эталонные копии (выход новых версий).
16.2. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.
16.3. Носители должны храниться в шкафу или помещении оборудованном системой пожаротушения.
16.4. Носители должны храниться не менее года, для возможности восстановления данных.
16.5. Резервирование и восстановление производится лицом, уполномоченным приказом по Гимназии.

17. ПОДБОР ПЕРСОНАЛА НА ДОЛЖНОСТЬ ОТВЕТСТВЕННЫХ ЛИЦ (АДМИНИСТРАТОР ИСПДН, ОТВЕТСТВЕННЫЙ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ

ДАННЫХ)

17.1. Из-за особых полномочий по доступу к персональным данным, обрабатываемых в Гимназии, подбор персонала на должность ответственных лиц должен осуществляться в особом порядке.

17.2. Основные профессиональные навыки, которыми должно обладать ответственное лицо:

17.2.1. выполнять сложные работы, связанные с обеспечением комплексной защиты информации на основе разработанных программ и методик, соблюдения конфиденциальности информации;

17.2.2. проводить сбор и анализ материалов учреждений, организаций и предприятий отрасли с целью выработки и принятия решений и мер по обеспечению защиты информации и эффективному использованию средств автоматического контроля, обнаружения возможных каналов утечки конфиденциальных сведений;

17.2.3. анализировать существующие методы и средства, применяемые для контроля и защиты информации, и разрабатывает предложения по их совершенствованию и повышению эффективности этой защиты;

17.2.4. участвовать в обследовании объектов защиты, их классификации и категорировании;

17.2.5. разрабатывать и подготавливать к утверждению проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;

17.2.6. организовать разработку и своевременное представление предложений для включения в соответствующие разделы перспективных и текущих планов работ и программ мер по контролю и защите информации;

17.2.7. давать отзывы и заключения на проекты вновь строящихся и реконструируемых зданий и сооружений и другие разработки по вопросам обеспечения защиты информации;

17.2.8. осуществлять проверку выполнения требований межотраслевых и отраслевых нормативных документов по защите информации;

17.2.9. знать нормативные требования по информационной безопасности средств информатизации;

17.2.10. знать перечень установленных в компании автоматизированных рабочих мест (далее АРМ) и перечень задач, решаемых с их использованием;

17.2.11. осуществлять учет и периодический контроль за составом и полномочиями пользователей, состоянием используемых средств защиты информации от несанкционированного доступа (далее СЗИ НСД), осуществлять проверку правильности их настройки (выборочное тестирование);

17.2.12. осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов;

17.2.13. проводить работу по выявлению возможных каналов вмешательства в процесс функционирования АС и осуществления НСД к информации и техническим средствам ПЭВМ;

17.2.14. вносить предложения директору Гимназии о совершенствовании СЗИ НСД.

18. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

18.1. Гимназия, а также должностные лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, гражданскую, административную, уголовную и иную ответственность, предусмотренную законодательством Российской Федерации.

Приложение 2

ЖУРНАЛ (форма)
учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных

№	ФИО субъекта, сведения о документе, удостоверяю щего личность	Дата обращения	Роспись субъекта	Цель	Отметка об исполнении	ФИО исполнителя	Роспись исполнителя

Приложение 3

УТВЕРЖДАЮ
Директор МБОУ «Гимназия № 2»

_____ _____
«___»_____ 20___ г.

АКТ (форма) № _____
уничтожении персональных данных

г. Инта «___» _____ 20___ г.

Комиссия составе:
председатель: _____

члены комиссии: _____

_____

_____

провела отбор носителей персональных данных и установила, что в соответствии с требованиями нормативных документов по защите информации данные, записанные на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего съемных носителей _____
(цифрами и прописью)
На указанных носителях персональные данные уничтожены путем
_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)
Перечисленные носители ПДн уничтожены путем
_____.
(разрезания, сжигания, механического уничтожения и т.п.)

Председатель комиссии: _____ _____
Члены комиссии:
_____ _____
_____ _____

Приложение 4

«___» _____ 20___ г.
№ _____

Ф.И.О. лица, подавшего запрос

на № _____
«___» _____ 20___ г.

СПРАВКА (форма)
об обработке персональных данных субъекта

_____.
(полное наименование Учреждения)

расположенное по адресу: _____
информирует об обработке персональных данных гр. _____.

1. Персональные данные указанного гражданина _____.
(обрабатываются/не обрабатываются)
2. Правовые основания обработки персональных данных: _____
_____
(ФЗ «О персональных данных», Трудовой кодекс РФ, ФЗ «Об образовании», ФЗ «Об архивном деле», другие)
_____
3. Цели обработки персональных данных: _____
_____.
4. Способы обработки персональных данных: _____
(автоматизированный/неавтоматизированный/ смешанный)
5. Кто имеет доступ, кому могут быть переданы персональные данные: _____
_____
(перечисляются другие операторы)
_____.
6. Обрабатываемые персональные данные: _____
_____
_____.
7. Источники получения персональных данных: _____
_____.
8. Сроки обработки и хранения персональных данных: _____
_____.
9. Порядок осуществления субъектом своих прав: согласно ФЗ «О персональных данных».
10. Трансграничная передача персональных данных: _____.
(осуществляется/не осуществляется)
11. Иные сведения: _____
_____.

Руководитель _____