Приложение 1

УТВЕРЖДЕНО
приказом директора СПб ГБУ «Центр содействия семейному воспитанию № 9»
от 25.01.2022 № 41-О

Положение о защите конфиденциальной информации
СПб ГБУ «Центр содействия семейному воспитанию № 9»

1. Общие положения

1.1. Положение о защите конфиденциальной информации СПб ГБУ «Центр содействия семейному воспитанию № 9» (далее соответственно – Положение, УЧРЕЖДЕНИЕ) регулирует отношения, связанные с обработкой конфиденциальной информации, создаваемой и (или) используемой в деятельности УЧРЕЖДЕНИЯ, в отношении которой УЧРЕЖДЕНИЕ является обладателем информации.

1.2. Для достижения цели в Положении определяются способы решения следующих задач:

1.2.1. определение конфиденциальной информации УЧРЕЖДЕНИЯ;

1.2.2. определения общих требований по обработке конфиденциальной информации;

1.2.3. определение разрешительной системы доступа к конфиденциальной информации, как основы ограничения доступа к конфиденциальной информации.

1.3. Основными принципами, которыми руководствуется УЧРЕЖДЕНИЕ в вопросах ограничения доступа к конфиденциальной информации, являются:

1.3.1. законность ограничения доступа – заключается в выполнении требований законодательства при отнесении информации (сведений, данных) к конфиденциальной информации. При этом учитываются как нормы, предписывающие налагать ограничения на доступ к этим сведениям, так и запрещающие такие ограничения;

1.3.2. обоснованность ограничения доступа – заключается в установлении путем экспертной оценки работниками УЧРЕЖДЕНИЯ отнесения информации к отдельным видам сведений, исходя из законных интересов УЧРЕЖДЕНИЯ и в соответствии с принятыми в УЧРЕЖДЕНИИ локальными нормативными актами;

1.3.3. своевременность ограничения доступа – заключается в установлении ограничений на разглашение и (или) распространение сведений с момента их получения (разработки) или заблаговременно.

1.4. В соответствии со статьей 6 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» действие Положения направлено на введение в УЧРЕЖДЕНИИ разрешительной системы доступа к конфиденциальной информации допускаемых лиц (далее – разрешительная система доступа).

1.5. Положение разработано в соответствии с Гражданским кодексом Российской Федерации, Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», иными нормативными правовыми актами Российской Федерации.

2. Основные понятия, используемые в Положении

В Положении используются следующие понятия:

2.1. **информация** – сведения (сообщения, данные) независимо от формы их представления (текстовая, числовая, графическая, аудио, видео, электронная), в том числе:

2.1.1. данные – сведения, зафиксированные в какой-либо форме;

2.1.2. сообщения – сведения в какой-либо форме, передаваемые между участниками информационного взаимодействия;

2.2. **документированная информация** – информация, зафиксированная на материальном носителе (в том числе на бумажной основе) путем документирования с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

2.3. **электронный документ** – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

2.4. **конфиденциальность информации** – требование не разглашать информацию третьим лицам без согласия ее обладателя, обязательное для выполнения лицом, получившим доступ к определенной информации;

2.5. **конфиденциальная информация** – сведения в любой объективной форме, доступ к которым ограничивается в соответствии с Положением и разглашение которых может нанести материальный, репутационный или иной ущерб интересам УЧРЕЖДЕНИЯ, его работников и воспитанников, и в отношении которой УЧРЕЖДЕНИЕМ введен режим конфиденциальности информации.

Возможными формами представления конфиденциальной информации являются:

2.5.1. речевая информация (информация, представленная в виде информативных акустических сигналов, которая озвучивается в том числе устно на встречах или совещаниях) и звуковая информация (информация, представленная в виде информативных акустических сигналов, которая озвучивается посредством звуковоспроизводящих устройств);

2.5.2. информация в электронной форме, размещаемая в информационных системах (обрабатывается на средствах вычислительной техники при помощи информационных технологий, представленная в виде информационных массивов, отдельных файлов и баз данных) и (или) передаваемая посредством информационно-телекоммуникационных систем (по каналам связи, локальным или глобальным вычислительным сетям);

2.5.3. недокументированная информация, зафиксированная на различных носителях (на бумажной, магнитной, оптической или другой основе);

2.5.4. документированная информация, зафиксированная на различных носителях (на бумажной, магнитной, оптической или другой основе);

2.5.5. документированная информация, размещаемая в информационных системах, в форме электронного документа.

2.6. **организация работы с документированной конфиденциальной информацией** – организация процессов учета, воспроизведения (копирования), предоставления, исполнения, отправления, классификации, систематизации, подготовки для оперативного и архивного хранения, уничтожения, хранения, проверки наличия и сохранности документированной конфиденциальной информации;

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

2.8. **информация, составляющая коммерческую тайну** – техническая, производственная, финансово-экономическая, коммерческая или иная информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, и позволяет ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение или получить преимущество на рынке товаров, работ, услуг или получить иную коммерческую выгоду, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим ограничения доступа;

2.9. **иные сведения конфиденциального характера УЧРЕЖДЕНИЯ** – сведения в любой объективной форме, создаваемые и используемые работниками УЧРЕЖДЕНИЯ, а также физическими лицами – исполнителями по гражданско-правовым договорам, при исполнении трудовых (функциональных) обязанностей;

2.10. **обладатель информации** – юридическое лицо (УЧРЕЖДЕНИЕ или его контрагент) или физическое лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

2.11. **допуск к конфиденциальной информации** – выполнение обладателем информации (уполномоченными должностными лицами) определенных процедур, связанных с оформлением права на доступ допускаемых лиц к конфиденциальной информации. Получение допуска со стороны допускаемого лица носит добровольный характер и является подтверждением с его стороны выполнения налагаемых обязательств. Наличие допуска предоставляет допускаемому лицу право работать с конфиденциальной информацией в объеме, определяемом обладателем информации;

2.12. **доступ к конфиденциальной информации** – практическая реализация предоставленного допуском права на возможность получения информации и ее использование (получение возможности ознакомления, в том числе с помощью технических средств, обработки, в частности, копирования, модификации или уничтожения);

2.13. **разрешительная система доступа** – совокупность правовых норм и требований, устанавливаемых обладателем информации с целью обеспечения правомерного ознакомления допускаемыми лицами с конфиденциальной информацией и ее использования для выполнения функциональных обязанностей. Разрешительная система доступа допускаемых лиц предусматривает установление в УЧРЕЖДЕНИИ единого порядка обращения с носителями сведений, составляющих конфиденциальную информацию, определение ограничений на доступ к ним различных категорий работников и иных допускаемых лиц, и степени ответственности за сохранность указанных носителей сведений.

2.14. **разглашение конфиденциальной информации** – действие или бездействие, в результате которых конфиденциальная информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя конфиденциальной информации;

2.15. **уничтожение конфиденциальной информации** – действия, направленные на приведение конфиденциальной информации в состояние, исключающее возможность ее использования и восстановления, в том числе посредством физического уничтожения и/ или удаления из памяти электронно-вычислительных машин носителей конфиденциальной информации и их копий;

2.16. **утрата конфиденциальной информации** – наносящее ущерб УЧРЕЖДЕНИЮ состояние конфиденциальной информации, к которому приводят хищение и/или потеря носителя конфиденциальной информации, несанкционированное уничтожение носителей конфиденциальной информации или только отображенной в них конфиденциальной информации, искажение или блокирование конфиденциальной информации;

2.17. **утечка конфиденциальной информации** – неправомерный (неразрешенный) выход такой информации за пределы защищаемой зоны ее функционирования в УЧРЕЖДЕНИИ или установленного круга лиц, имеющих право работать с ней, если этот выход привел к получению информации (ознакомлению с ней) лицами, не имеющими к ней санкционированного доступа. К утечке конфиденциальной информации приводит, в том числе, ее несанкционированное разглашение или распространение;

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

2.19. **информационные ресурсы** – совокупность данных, организованных для получения информации. Под информационными ресурсами подразумеваются отдельные

документы, массивы документов, базы данных в информационных системах, архивах, хранилищах, в том числе на носителях информации;

2.20. **несанкционированный доступ** – доступ к информации, нарушающий правила разграничения доступа с использованием или без использования штатных средств информационных систем;

2.21. **работник УЧРЕЖДЕНИЯ** – физическое лицо, вступившее в трудовые отношения с учреждением;

2.22. **воспитанник** – физическое лицо, принятое приказом в контингент учреждения.

3. Порядок отнесения информации к категории конфиденциальной

3.1. Конфиденциальной информацией УЧРЕЖДЕНИЯ признаются следующие сведения:

3.1.1. Персональные данные, обрабатываемые УЧРЕЖДЕНИЕМ;

3.1.2. Иные сведения конфиденциального характера, признанные УЧРЕЖДЕНИЕМ как подлежащие защите, и разглашение которых может нанести материальный, репутационный или иной ущерб УЧРЕЖДЕНИЮ, его работникам и воспитанникам, в том числе указанные в Приложении 1 к Положению.

3.2. Ограничение доступа не может быть установлено в отношении следующих сведений:

3.2.1.содержащихся в учредительных документах УЧРЕЖДЕНИЯ, документах, подтверждающих факт внесения записей о УЧРЕЖДЕНИИ в соответствующий государственный реестр;

3.2.2.о составе имущества УЧРЕЖДЕНИЯ и об использовании средств соответствующих бюджетов;

3.2.3.о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

3.2.4.о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

3.2.5.о задолженности по выплате заработной платы и социальным выплатам;

3.2.6.о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

3.2.7.о перечне лиц, имеющих право действовать без доверенности от имени УЧРЕЖДЕНИЯ;

3.2.8.обязательность раскрытия которых или недопустимость ограничения доступа, к которым установлена федеральными законами.

3.3. Отношения УЧРЕЖДЕНИЯ и физических лиц, возникающие в связи с обработкой их персональных данных в УЧРЕЖДЕНИИ, регулируются Положением о защите персональных данных УЧРЕЖДЕНИЕМ.

3.4. Сводный перечень сведений конфиденциального характера УЧРЕЖДЕНИЯ представлен в Приложении 1 к Положению. Руководители структурных подразделений, в деятельности которых присутствуют процессы обработки конфиденциальной информации, имеют право на подачу заявки на актуализацию указанного перечня.

3.5. Сведения, которые были получены УЧРЕЖДЕНИЕМ от третьих лиц и в отношении которых третьими лицами заявлено, что они являются их конфиденциальной информацией, или конфиденциальный характер которых следует из законодательства Российской Федерации, подлежат защите наряду с конфиденциальной информацией УЧРЕЖДЕНИЯ.

3.6. Режим конфиденциальности информации УЧРЕЖДЕНИЯ действует:

3.6.1. для персональных данных, обрабатываемых УЧРЕЖДЕНИЕМ, – до прекращения деятельности УЧРЕЖДЕНИЯ;

3.6.2. для информации, полученной от контрагентов УЧРЕЖДЕНИЯ, – в течении срока, определенного соглашением о неразглашении конфиденциальной информации или иным договором.

4. Общие требования по обработке конфиденциальной информации

4.1. Обработка конфиденциальной информации включает в себя процессы подготовки и изготовления конфиденциальной информации, организации работы с конфиденциальной информацией и защиты конфиденциальной информации.

4.2. В УЧРЕЖДЕНИИ, в зависимости от форм представления конфиденциальной информации, регламентируются следующие направления обработки конфиденциальной информации:

4.2.1. обработка речевой и (или) звуковой конфиденциальной информации;

4.2.2. обработка недокументированной конфиденциальной информации:

– в электронной форме, размещенной в информационных системах или передаваемой посредством информационно-телекоммуникационных систем;

– зафиксированной на различных носителях (на бумажной, магнитной, оптической или другой основе);

4.2.3. обработка документированной конфиденциальной информации:

– размещенной в информационных системах в форме электронного документа;

– зафиксированной на различных носителях (на бумажной, магнитной, оптической или другой основе).

4.3. Требования к обработке конфиденциальной информации зависят от форм представления конфиденциальной информации и в части, не урегулированной Положением, регламентируются отдельными локальными нормативными актами.

4.4. Деятельность, связанная с обработкой конфиденциальной информации в УЧРЕЖДЕНИИ, должна включать в себя, в том числе, мероприятия по защите конфиденциальной информации от утраты и утечки.

5. Разрешительная система доступа к конфиденциальной информации

5.1. Разрешительная система доступа является частью системы правовых, организационных, технических и иных мер, принимаемых УЧРЕЖДЕНИЕМ к защите конфиденциальной информации.

5.2. Разрешительная система доступа предназначена для решения следующих задач:

5.2.1. определение участников разрешительной системы доступа;

5.2.2. определение условий предоставления доступа и порядка допуска к конфиденциальной информации;

5.2.3. определение порядка работы с конфиденциальной информацией;

5.2.4. определение обязанностей лиц в рамках соблюдения разрешительной системы доступа;

5.2.5. определение степени ответственности лиц.

5.3. Принципы построения разрешительной системы доступа:

5.3.1. надежность, реализуемая принятием мер по исключению возможности несанкционированного доступа посторонних лиц к конфиденциальной информации в обычных и экстремальных условиях;

5.3.2. полнота охвата всех категорий исполнителей и всех категорий конфиденциальной информации;

5.3.3. конкретность, т.е. исключение двоякого толкования, и однозначность решения о допуске к конфиденциальной информации;

5.3.4. производственная необходимость как единственный критерий доступа исполнителя к конфиденциальной информации, а также доступа к конфиденциальной

информации представителей органов власти в случаях, определяемых законодательством Российской Федерации;

5.3.5. определенность состава и компетенции должностных лиц, дающих разрешение на доступ исполнителя к конфиденциальной информации, исключение возможности бесконтрольной и несанкционированной выдачи таких разрешений;

5.3.6. строгая регламентация порядка работы с конфиденциальной информацией.

6. Участники разрешительной системы доступа в УЧРЕЖДЕНИИ

6.1. К лицам, имеющим доступ к конфиденциальной информации без прохождения процедуры допуска в силу должностных обязанностей и ответственным за организацию разрешительной системы доступа в УЧРЕЖДЕНИИ относятся:

6.1.1. директор;
6.1.2. заместители директора;
6.1.3. главный бухгалтер;
6.1.4. заведующие отделений;
6.1.5. специалист по кадрам;
6.1.6. специалист по закупкам;
6.1.7. медицинские работники;
6.1.8. социальные педагоги;
6.1.9. педагоги-психологи;
6.1.10. воспитатели.

6.2. Директор, заместители директора, главный бухгалтер, заведующие отделений УЧРЕЖДЕНИЯ могут делегировать сотрудникам координируемых структурных подразделений часть своих полномочий в части допуска к конфиденциальной информации в установленном в УЧРЕЖДЕНИИ порядке.

6.3. Под допускаемыми к конфиденциальной информации лицами в УЧРЕЖДЕНИИ понимаются:

6.3.1. работники УЧРЕЖДЕНИЯ;

6.3.2. лица, выполняющие работу или оказывающие услуги на основании гражданско-правовых договоров с УЧРЕЖДЕНИЕМ;

6.3.3. иные лица (в том числе контрагенты или представители государственных органов).

7. Условия предоставления доступа и порядок допуска к конфиденциальной информации

7.1. Предоставление доступа к конфиденциальной информации возможно в следующих случаях:

7.1.1. конфиденциальная информация необходима для выполнения трудовых обязанностей (в том числе указанных в должностных инструкциях) допускаемых лиц из числа работников УЧРЕЖДЕНИЯ;

7.1.2. конфиденциальная информация необходима для выполнения договорных обязательств допускаемыми лицами из числа указанных в подпунктах 6.3.2, 6.3.3 пункта 6.3 Положения;

7.1.3. конфиденциальная информация УЧРЕЖДЕНИЕ необходима для подготовки ответа уполномоченным лицом структурного подразделения УЧРЕЖДЕНИЕ на запросы органов государственной власти, иных государственных органов, органов местного самоуправления о предоставлении конфиденциальной информации.

7.2. Работники УЧРЕЖДЕНИЯ, которым для выполнения своих трудовых обязанностей необходимо иметь доступ к конфиденциальной информации, если такая необходимость возникла как при приеме на работу, так и в период работы в УЧРЕЖДЕНИИ, должны быть ознакомлены с настоящим Положением, перечнем конфиденциальной информации УЧРЕЖДЕНИЯ, предупреждены об ответственности за разглашение сведений,

содержащих конфиденциальную информацию, и должны дать письменное обязательство о неразглашении указанных сведений в соответствии с примерной формой, приведенной в Приложении 2 или Приложении 3 к Положению[1].

7.3. Руководители структурных подразделений разъясняют допускаемым лицам из числа работников (в том числе поступающим на работу) особенности порядка обращения с конфиденциальной информацией, том числе с персональными данными. Инструктаж проводится в объеме Положения и других нормативных правовых и локальных нормативных актов, регламентирующих обеспечение сохранности конфиденциальной информации, в том числе персональных данных.

7.4. Допускаемые работники получают доступ в объеме, необходимом для выполнения ими своих трудовых обязанностей, с разрешения руководителя структурного подразделения и на основании прохождения процедуры допуска.

7.5. Лица из числа указанных в подпункте 6.3.2 пункта 6.3 Положения, допускаемые к конфиденциальной информации, принимают на себя обязательства о неразглашении полученной конфиденциальной информации по форме, которая приведена в Приложении 4 к Положению; лица из числа указанных в подпункте 6.3.3 пункта 6.3 Положения, допускаемые к конфиденциальной информации, принимают на себя обязательства о неразглашении полученной конфиденциальной информации по форме, которая приведена в Приложении 5 к Положению.

7.6. Условия доступа представителей органов государственной власти, иных государственных органов, органов местного самоуправления или условия предоставления конфиденциальной информации УЧРЕЖДЕНИЯ по запросам указанных органов определяются в соответствии с законодательством РФ.

7.7. Процесс допуска к конфиденциальной информации направлен на исключение необоснованного расширения круга лиц, допускаемых к конфиденциальной информации, и утечки этой информации, а также доступа к ней лиц, не имеющих на то разрешения полномочных должностных лиц УЧРЕЖДЕНИЯ.

7.8. Лица, которым необходимо работать с конфиденциальной информацией, могут быть допущены к конфиденциальной информации в случае, если они заявили о необходимости доступа к конфиденциальной информации, относятся к категории допускаемых лиц, прошли процедуру допуска, являющуюся составной частью разрешительной системы доступа к конфиденциальной информации УЧРЕЖДЕНИЯ.

7.9. Процедуру допуска имеет право провести должностное лицо УЧРЕЖДЕНИЯ, указанное в пунктах 6.1, 6.2 Положения в пределах своей компетенции.

7.10. Процедура допуска предусматривает в обязательном порядке выполнение следующих мероприятий:

7.10.1. проверка отнесения допускаемого лица к категории допускаемых лиц в соответствии с пунктом 6.3 Положения;

7.10.2. проверка выполнения условий предоставления доступа в соответствии с пунктами 7.1 – 7.7 Положения;

7.10.3. выдача разрешения на доступ к конфиденциальной информации;

7.10.4. организация учета допущенных лиц и сведений конфиденциального характера в журнале учета лиц по форме, которая приведена в Приложении 6 к Положению.

7.11. Права допускаемых лиц на доступ к конфиденциальной информации регулируются разрешениями указанных должностных лиц, оформленными в документальном

---

[1] Выбор используемой формы (Приложение 2 или Приложение 3) осуществляется руководителем структурного подразделения работника, исходя, в том числе, из следующей рекомендации: форма соглашения (Приложение 2) используется, если работнику предоставляется доступ к конфиденциальной информации, риски распространения которой и/или потенциальный вред от разглашения которой являются значительными, и/ или если работник привлекается к исполнению обязательств УЧРЕЖДЕНИЯ перед третьими лицами по договору; форма обязательства (Приложение 3) используется, когда работнику предоставляется доступ к менее значимой конфиденциальной информации.

(письменном или электронном) виде в отношении непосредственно подчиненных им лиц, в соответствии с пунктом 7.10 Положения.

7.12. В УЧРЕЖДЕНИИ применяются следующие способы документального оформления разрешений на доступ к конфиденциальной информации (формы разрешительных документов):

7.12.1. составление именных (должностных) списков лиц, допускаемых к той или иной конфиденциальной информации УЧРЕЖДЕНИЯ, в обязательном порядке содержащих должности и фамилии лиц и категории сведений (документов), к которым они допускаются, согласно перечню Приложения 1 к Положению;

7.12.2. составление именных (должностных) списков лиц, допускаемых к ресурсам информационных систем, содержащих конфиденциальную информацию УЧРЕЖДЕНИЯ, в обязательном порядке содержащих должности и фамилии лиц, наименование ресурсов (информации, документов, баз данных), к которым они допускаются, и прав по доступу;

7.12.3. оформление разрешения непосредственно на документе (носителе информации) в виде резолюции (поручения), адресованного конкретному лицу;

7.12.4. указание (перечисление) в организационно-распорядительных и иных документах УЧРЕЖДЕНИЯ лиц (их фамилий), которые при решении конкретных производственных и иных задач должны быть допущены к определенной информации, составляющей конфиденциальную информацию УЧРЕЖДЕНИЯ.

8. Порядок работы с конфиденциальной информацией

8.1. Доступ к конфиденциальной информации предусматривает возможность ознакомления с ней и ее обработку, которая заключается в выполнении следующих действий (операций):

8.1.1. чтение (ознакомление);

8.1.2. копирование, хранение, использование, передачу, удаление (уничтожение).

8.2. Предоставление конфиденциальной информации третьим лицам, в том числе органам государственной власти, иным государственным органам, органам местного самоуправления осуществляется по распоряжению руководителя структурного подразделения.

8.3. В случае возникновения необходимости передать конфиденциальную информацию третьему лицу, должно быть получено разрешение руководителя структурного подразделения, в деятельности которого получена соответствующая конфиденциальная информация.

8.4. При передаче конфиденциальной информации контрагенту УЧРЕЖДЕНИЯ разрешается использовать только способ, указанный в соглашении о неразглашении конфиденциальной информации, заключенном УЧРЕЖДЕНИЕМ с соответствующим контрагентом.

9. Обязанности лиц в рамках разрешительной системы доступа

9.1. Лица, имеющие доступ к конфиденциальной информации, обязаны:

9.1.1. сохранять конфиденциальность информации, к которой они были допущены, обеспечить неразглашение сведений, составляющих конфиденциальную информацию УЧРЕЖДЕНИЯ, в публикациях, докладах, документации, при экспонировании на выставках, в ходе организационно-технических переговоров, служебных и неслужебных разговоров, а равно любым иным способом;

9.1.2. при работе с конфиденциальной информацией выполнять требования по защите информации, изложенные в локальных нормативных актах УЧРЕЖДЕНИЯ по обеспечению информационной безопасности, в том числе сохранять в тайне свой индивидуальный пароль от компьютерной техники и сервисов, входящих в состав личного кабинета, и периодически менять его;

9.1.3. при прекращении или расторжении трудового договора передать руководителю

соответствующего структурного подразделения материальные носители, содержащие конфиденциальную информацию;

9.1.4. сообщать своему непосредственному руководителю или лицу, его замещающему, об утрате или недостаче документов, содержащих конфиденциальную информацию, ключей от сейфов (хранилища), печатей, удостоверений, пропусков, а также о любых иных обстоятельствах, создающих угрозу конфиденциальности информации;

9.1.5. при возникновении необходимости в передаче конфиденциальной информации по электронной почте не осуществлять передачу конфиденциальной информации с использованием иных средств, чем электронная почта УЧРЕЖДЕНИЯ (если иное не предусмотрено в отдельном соглашении или обязательстве о неразглашении);

9.1.6. при передаче конфиденциальной информации в электронной форме по электронной почте УЧРЕЖДЕНИЯ включить в исходящее письмо и в последующую переписку уведомление о конфиденциальности в следующей форме:

- на русском языке: «Это электронное сообщение и любые документы, приложенные к нему, содержат конфиденциальную информацию и предназначены исключительно для использования работниками УЧРЕЖДЕНИЯ, физическим или юридическим лицом, которому они адресованы. Уведомляем Вас о том, что, если это сообщение не предназначено Вам, использование, копирование, распространение информации, содержащейся в настоящем сообщении, а также осуществление любых действий на основе этой информации, не допускается. Если Вы считаете, что Вы получили это электронное сообщение по ошибке, пожалуйста, свяжитесь с отправителем и незамедлительно удалите электронное сообщение и любые вложения с компьютера. Заранее благодарим.»;

9.2. Лицам, имеющим доступ к конфиденциальной информации, запрещается:

9.2.1. разглашать конфиденциальную информацию (в том числе знакомить с документами и (или) электронными документами, содержащими конфиденциальную информацию) любым лицам, кроме лиц, допущенных к конфиденциальной информации;

9.2.2. размещать конфиденциальную информацию в сети Интернет;

9.2.3. использовать конфиденциальную информацию в передачах по радио и телевидению, в публичных выступлениях;

9.2.4. снимать копии с документов и других носителей информации, содержащих конфиденциальную информацию, производить выписки из них, а равно использовать различные технические средства (фото-, видео- и звукозаписывающую аппаратуру) для регистрации сведений без разрешения руководителя соответствующего структурного подразделения;

9.2.5. осуществлять пересылку конфиденциальной информации, на личные адреса средств коммуникации (электронная почта, мессенджеры, программные средства социальных сетей и т.п.);

9.2.6. использовать без разрешения от непосредственного руководителя и согласования представителя Центра информационной безопасности для хранения и обработки конфиденциальной информации личные ноутбуки, карманные персональные компьютеры, фотоаппараты, видеокамеры, электронные записные книжки, смартфоны, мобильные телефоны и другие цифровые (вычислительные) устройства, имеющие возможность ввода, хранения, накопления, приема, передачи информации[2];

9.2.7. самовольно подключать периферийные устройства[3] или устанавливать дополнительные любые программные средства, копировать конфиденциальную информацию на личные флеш-карты и иные устройства хранения информации;

9.2.8. использовать для хранения конфиденциальной информации облачные сервисы, за исключением сервисов, контролируемых УЧРЕЖДЕНИЕМ.

---

[2] Исключения из этого правила допускаются исключительно для научно-педагогических работников по решению руководителя структурного подразделения, в котором работает работник.

[3] Под периферийным устройством необходимо понимать внешние по отношению к системному блоку компьютера устройства (USB-флеш, внешний CD-ROM, внешний жесткий диск, VPN-ключ, e-token).

9.3. Лица, имеющие доступ к конфиденциальной информации, обязаны:

9.3.1. не создавать копии (в том числе электронные) конфиденциальной информации (в том числе на отделяемые (внешние) носители информации) без получения предварительного согласия руководителя соответствующего структурного подразделения;

9.3.2. определять количество экземпляров документов (в том числе электронных), содержащих конфиденциальную информацию, в строгом соответствии с действительной необходимостью;

9.3.3. использовать при работе с конфиденциальной информацией УЧРЕЖДЕНИЯ, контрагента УЧРЕЖДЕНИЯ только средства вычислительной техники (стационарные компьютеры, мобильные устройства), оснащенные средствами защиты, достаточными для обеспечения информационной безопасности в соответствии с требованиями локальных актов, определяющих политику информационной безопасности УЧРЕЖДЕНИЯ;

9.3.4. прекратить обработку конфиденциальной информации на компьютерной технике при обнаружении в последней неисправностей, вирусов, шпионских программ, программ-майнеров, других вредоносных программ и сообщить о выявленных неисправностях своему непосредственному руководителю (или лицу, его замещающему) и представителю Центра информационной безопасности.

9.4. Ответственными за обеспечение режима конфиденциальности информации в структурных подразделениях УЧРЕЖДЕНИЯ являются руководители соответствующих структурных подразделений.

9.5. При получении УЧРЕЖДЕНИЕМ информации, в отношении которой требуется установление режима конфиденциальности, руководитель структурного подразделения, в деятельности которого получена соответствующая информация, обеспечивает принятие всех необходимых мер по установлению и поддержанию режима конфиденциальности информации, указанных в Положении. Если конфиденциальная информация была получена в деятельности нескольких подразделений, меры по установлению и поддержанию режима конфиденциальности информации применяются совместно руководителями указанных подразделений.

9.6. В целях поддержания режима конфиденциальности информации руководитель структурного подразделения в том числе:

9.6.1. обеспечивает учет лиц, получивших доступ к конфиденциальной информации, и (или) лиц, которым такая информация была предоставлена или передана;

9.6.2. уведомляет работника, доступ которого к конфиденциальной информации необходим для выполнения им своих трудовых обязанностей, о конфиденциальном характере раскрываемой работнику информации, обладателями которой являются УЧРЕЖДЕНИЕ или его контрагенты;

9.6.3. контролирует факт ознакомления под подпись работника с Положением и иными локальными нормативными актами, направленными на обеспечение конфиденциальности информации в УЧРЕЖДЕНИИ и с мерами ответственности за их нарушение;

9.6.4. создает работнику необходимые условия для соблюдения им установленного УЧРЕЖДЕНИЕМ режима конфиденциальной информации;

9.6.5. обеспечивает заключение с контрагентами УЧРЕЖДЕНИЯ, в том числе с лицами, выполняющими работы (оказывающими услуги) в пользу УЧРЕЖДЕНИЯ на основании гражданско-правовых договоров, соглашений о неразглашении конфиденциальной информации;

9.6.6. исполняет иные обязанности, предусмотренные Положением.

9.7. Если информация, в отношении которой целесообразно установление режима конфиденциальности информации, получена в ходе выполнения работ по договору или реализации соглашения, в целях определения конкретных сведений, подлежащих охране, необходимых мер по защите информации, а также для урегулирования иных вопросов, руководитель подразделения, ответственный за исполнение договора (соглашения) со

стороны УЧРЕЖДЕНИЯ, обеспечивает включение в соответствующий договор (соглашение) положений, определяющих взаимные обязательства и ответственность сторон за ее сохранность.

9.8. В случае, если обладателем конфиденциальной информации является контрагент УЧРЕЖДЕНИЯ, в договоре с которым предусмотрена обязанность УЧРЕЖДЕНИЯ уведомить контрагента о факте предоставления информации в ответ на основанное на законе требование органа государственной власти, иного государственного органа, органа местного самоуправления, руководитель структурного подразделения УЧРЕЖДЕНИЯ, ответственный за исполнение договора, обеспечивает направление контрагенту соответствующего уведомления в случаях, когда данные действия не будут являться нарушением требований применимого законодательства.

10. Ответственность за нарушение режима конфиденциальности информации

10.1. Ответственность за нарушение режима конфиденциальности основывается на принципе персональной ответственности, который заключается в том, что каждое лицо, разрешающее доступ или получившее доступ к конфиденциальной информации должно лично отвечать за свою деятельность, включая любые действия с конфиденциальной информацией и возможные нарушения по обеспечению ее безопасности, т.е. какие-либо случайные или умышленные действия, которые приводят или могут привести к несанкционированной утечке или утрате конфиденциальной информации.

10.2. Лица, разгласившие конфиденциальную информацию, или иным образом нарушившие установленную Положением разрешительную систему доступа, работы и хранения к конфиденциальной информации, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

10.3. Нарушением режима конфиденциальности информации признаются, в том числе:

10.3.1. разглашение конфиденциальной информации;

10.3.2. неправомерное использование конфиденциальной информации;

10.3.3. несанкционированный доступ к конфиденциальной информации;

10.3.4. утрата документов и иных материальных носителей, содержащих конфиденциальную информацию;

10.3.5. неправомерное уничтожение документов, содержащих конфиденциальную информацию;

10.3.6. нарушение требований хранения документов, содержащих конфиденциальную информацию;

10.3.7. другие нарушения требований законодательства и настоящего Положения.

Приложение 1
к Положению о защите конфиденциальной информации
СПб ГБУ «Центр содействия семейному воспитанию № 9»

Перечень конфиденциальной информации
СПб ГБУ «Центр содействия семейному воспитанию № 9»

№	Направления деятельности	Лица, уполномоченные на распоряжение конфиденциальной информацией	Основные категории конфиденциальной информации
1	По всем направлениям деятельности	Директор Заместители директора Руководители структурных подразделений	1. Информация о хозяйственно-финансовых отношениях с деловыми партнерами (в том числе условия договорных отношений с ними), о проведении переговоров, переписке с ними; 2. информация, составляющая электронную базу УЧРЕЖДЕНИЯ, содержащая сведения об обучающихся, работниках, деловых партнерах УЧРЕЖДЕНИЯ; 3. не являющаяся общедоступной информация о деятельности УЧРЕЖДЕНИЯ; 4. условия сделок, за исключением существенных, которые имеют гласный характер, т. е. подлежат обязательному доведению до сведения любых заинтересованных лиц; 5. сведения о контрагентах УЧРЕЖДЕНИЯ (в т.ч. состояние расчетов с контрагентами, включая активы контрагентов; состав поручений контрагентов); которые не содержатся в открытых источниках (справочниках, каталогах и др.) или переданы в УЧРЕЖДЕНИЕ указанными лицами на доверительной основе (в том числе адреса, телефоны, сведения об имущественных правах, аффилированных лицах, деловых связях, финансовом и экономическом состоянии и т.п.) а также персональная информация о работниках; 6. сведения о подготовке, принятии и исполнении решений руководства по вопросам его деятельности, развития, а также по иным организационным и научно-техническим вопросам; 7. идентификаторы и пароли, используемые сотрудниками УЧРЕЖДЕНИЯ для доступа в служебные помещения, к информации в электронном виде; 8. содержание заключенных договоров (контрактов), информация, полученная УЧРЕЖДЕНИЕМ в рамках исполнения договора (контракта) и определенная раскрывающей стороной как конфиденциальная, за исключением информации, подлежащей обнародованию и предоставлению третьим лицам во исполнение требований действующего законодательства; 9. сведения о совещаниях, проводимых в УЧРЕЖДЕНИИ, и содержание обсуждаемой на таких совещаниях информации, при условии, что до начала совещания или во время проведения совещания было сделано предупреждение в любой форме о конфиденциальности такого совещания;

			10. информация о личных отношениях работников как между собой, так и с руководством, сведения о возможных противоречиях, конфликтах внутри коллектива;
2	Деятельность по общему делопроизводству (то есть за исключением кадрового делопроизводства)	Документовед	1. информация о системе делопроизводства и документооборота УЧРЕЖДЕНИЯ; 2. оперативные (текущие) документы общего делопроизводства: внутренние (организационные, распорядительные, информационно-справочные и др.); 3. входящая (за исключением входящих рекламных предложений) и исходящая корреспонденция (в том числе в электронном виде) 4. информация, отмеченная грифом «для служебного пользования».
3	Деятельность по ведению архива УЧРЕЖДЕНИЯ	Документовед в рамках своих должностных компетенций	1. информация о системе архивного хранения и использования архивных документов УЧРЕЖДЕНИЯ; 2. архивные документы кадрового делопроизводства
5	Деятельность по обеспечению безопасности	Заведующий хозяйством Инженер по ГО и ЧС Специалист по охране труда	1. Сведения о порядке и состоянии организации безопасности и системе охраны, пропускном режиме, противопожарной безопасности, систем сигнализации (охранной и АПС) и т.п. 2. Переписка с правоохранительными органами, структурными подразделениями МЧС России, Департаментом ГОЧС и ПБ. 3. Материалы расследований и разбирательств. 4. Документы по учету нарушений. 5. Документы внешнего и внутреннего аудита. 6. Материалы по профилактике распространения и потребления ПАВ.
6	Закупочная деятельность	Специалист по закупкам	1. Сведения о готовящихся торгах, и документация о таких торгах до их объявления.
7	Деятельность по связям с общественностью	Специалист по связям с общественностью	1. Финансовое планирование УЧРЕЖДЕНИЯ; 3.Сведения о планах УЧРЕЖДЕНИЯ в отношении формирования публичной информационной политики (а именно: детали внутренних графиков встреч, мероприятий, в отношении которых руководство УЧРЕЖДЕНИЯ приняло решение не информировать общественность)
8	Деятельность по подбору персонала и кадровая работа	Специалист по кадрам	1. Сведения о размере заработной платы; сведения о принятии решений, касающихся материального стимулирования работников, в том числе о процедуре их согласования; 2. Положения трудовых договоров (контрактов), заключаемых с работниками, за исключением сведений, которые не могут относиться к конфиденциальной информации в соответствии с законодательством Российской Федерации; 3. Система организации труда, за исключением информации, подлежащей обнародованию и предоставлению третьим лицам во исполнение требований действующего законодательства

9	Финансовая и бухгалтерская деятельность	Главный бухгалтер Бухгалтер Экономист	1. Финансовая информация, имеющая коммерческую ценность, не содержащаяся в учредительных и иных документах, находящихся в публичном доступе, а также относящаяся к категории ограниченного доступа, в том числе: - персональная информация физических лиц; - образцы подписей физических лиц; - документы, содержащие сведения о получаемых и предлагаемых предложениях; - деловая переписка; - протоколы закрытых совещаний; - информация, содержащаяся в регистрах бухгалтерского учета и внутренней бухгалтерской отчетности; - данные налогового учета и налоговой отчетности; - сведения об исполнении договоров, контрактов и соглашений; - данные первичных учетных документов; - персональная информация физических лиц; - штатная расстановка с указанием ФИО и оплаты труда работников; - информация, содержащаяся в регистрах внутренней финансовой отчетности; - договоры, контракты и соглашения, сведения об их исполнении; - сведения, касающиеся предмета договоров на выполнение научно-исследовательских работ, хода их исполнения и полученных результатов, если иное не предусмотрено договорами; - персональная информация физических лиц.
10	Деятельность по цифровизации процессов УЧРЕЖДЕНИЯ и обеспечению информационной безопасности	Администратор системный	Реквизиты административного доступа к серверному, сетевому оборудованию, системам хранения данных, системам управления средой виртуализации и корпоративным информационным системам. 1. Реквизиты административного доступа к системам защиты информации. 2. Сведения, содержащиеся в материалах, описывающих следующие направления обеспечения информационной безопасности, и которые могут быть использованы в дальнейшем для противоправных действий по нанесению ущерба УЧРЕЖДЕНИЮ: – о проектных решениях по обеспечению защиты информации при разработке, модернизации и эксплуатации корпоративных информационных систем; – о результатах комплексных проверок эффективности системы защиты информации корпоративных информационных систем до утверждения акта (заключения) по проверке; – о результатах анализа проведенных расследований инцидентов информационной безопасности.
11	Деятельность по правовому сопровождению	Юрисконсульт	1. Персональная информация физических лиц; 2. информация, ставшая известной при подготовке материалов по результатам рассмотрения актов органов власти и служебных проверок, переписка с правоохранительными органами, материалы расследований и разбирательств;

			3. информация об УЧРЕЖДЕНИИ, ставшая известной в процессе рассмотрения претензий, жалоб, обращений, дисциплинарных производств, подготовки дела к судебному разбирательству, в процессе судебного разбирательства, по итогам судебного разбирательства (за исключением общедоступной информации); 4. правовые позиции по правовым вопросам, если они не были сделаны УЧРЕЖДЕНИЕМ общедоступными.