**МУНИЦИПАЛЬНОЕ КАЗЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

**«БЫКОВСКАЯ СРЕДНЯЯ ШКОЛА № 2»**

**БЫКОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ВОЛГОГРАДСКОЙ ОБЛАСТИ**

**404067, Волгоградская область, Быковский муниципальный район п.Зеленый, ул. Сиреневая 5, школа Тел. 8(84495)3-55-41 E-mail:** bkv_sh.2@volganet.ru

СОГЛАСОВАНО
Педагогическим советом
МКОУ «Быковская СШ № 2”

(протокол № 1 от 29.08.2025 г.)

УТВЕРЖДАЮ
И.о. директора
МКОУ «Быковская СШ № 2»
Быковского муниципального района»
_____ Е.А.Назирова
Приказ № 150-о/д от 29.08.2025 г.

# ПОЛОЖЕНИЕ О ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В МКОУ «БЫКОВСКАЯ СШ № 2» БЫКОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ВОЛГОГРАДСКОЙ ОБЛАСТИ

## 1. Общие положения

1.1. Настоящее Положение о защите конфиденциальной информации в Муниципальном казенном общеобразовательном учреждении «Быковская СШ № 2» Быковского муниципального района Волгоградской области (далее - Положение) разработано в соответствии с:

- Гражданским кодексом Российской Федерации (далее – ГК РФ),
- Трудовым кодексом Российской Федерации (далее – ТК РФ),
- 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 Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»,
- постановлением Правительства Российской Федерации от 05.12.1991 № 35 «О перечне сведений, которые не могут составлять коммерческую тайну»,
- постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
- приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,
- Уставом Муниципального казенного общеобразовательного учреждения «Быковская средняя школа №2» Быковского муниципального района Волгоградской области (далее – Центр, МКОУ «Быковская СШ №2»).

1.2. Положение определяет общий порядок обращения с конфиденциальной информацией (далее - информация).

1.3. Центр имеет право:

- определять состав, объем и порядок защиты конфиденциальной информации, персональных данных обучающихся, воспитанников, работников;
- требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

1.4. Центр обязан обеспечить сохранность конфиденциальной информации.

1.5. Информационные ресурсы, содержащие конфиденциальную информацию, сформированные в процессе деятельности Центра, а также приобретенные в собственность Центра установленными законодательством Российской Федерации способами, являются собственностью МКОУ «Быковская СШ №2» Быковского муниципального района

и не могут быть использованы иначе как с разрешения собственника и (или) в установленных законом случаях.

1.6. К конфиденциальной информации относятся данные, разглашение которых может нанести материальный, моральный или иной ущерб интересам Центра, его работников, обучающихся, воспитанников, их родителей (законных представителей).

Информация конфиденциального характера не может быть использована в целях затруднения реализации прав и свобод граждан.

1.7. Отнесение информации к конфиденциальной осуществляется в порядке, установленном законодательством Российской Федерации.

Для определения конфиденциальности сведений в МКОУ «Быковская СШ №2» используется Сводный перечень сведений конфиденциального характера (приложение к настоящему Положению).

Конфиденциальность документов, составленных на основании материалов, поступивших из других организаций, определяется степенью конфиденциальности сведений, содержащихся в этих материалах.

1.8. Под защитой информации подразумевается:

- деятельность, направленная на предотвращение утечки конфиденциальной информации, несанкционированных и непреднамеренных воздействий на конфиденциальную информацию;
- комплекс административных, организационных и технических мероприятий, направленных на ограничение доступа к информации и ее носителям в целях обеспечения ее сохранности и недоступности третьим сторонам, предусмотренных законодательством Российской Федерации;
- привлечение лиц, нарушающих режим конфиденциальной информации Центра, к установленной ответственности.

1.9. Защита конфиденциальной информации предусматривает:

- определение конфиденциальной информации, и сроков ее защиты;
- систему допуска сотрудников Центра, третьих лиц к конфиденциальной информации;
- обязанности лиц, допущенных к конфиденциальной информации;
- порядок работы с бумажными документами, содержащими конфиденциальную информацию;
- порядок работы с электронными документами, содержащими конфиденциальную информацию;
- обеспечение сохранности документов и дел (архивов) содержащих конфиденциальную информацию;
- принципы организации и проведения контроля за обеспечением установленного порядка при работе с конфиденциальной информацией;
- ответственность за разглашение конфиденциальной информации и утрату документов, содержащих конфиденциальную информацию.

1.10. Законодательством Российской Федерации:

1.10.1. Запрещено относить к информации конфиденциального характера:

- законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

- документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

- документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к государственной тайне;

- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

1.10.2. Установлено, что коммерческую тайну не могут составлять: - учредительные документы и Устав,

- документы, подтверждающие факт внесения записей о юридическом лице в Единый государственный реестр юридических лиц;

- лицензии, свидетельства о государственной аккредитации;

- сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему Российской Федерации; - документы о платежеспособности;

- сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

- документы об уплате налогов и обязательных платежах;

- сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, а также других нарушениях законодательства Российской Федерации и размерах причиненного при этом ущерба;

- сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

## 2. Порядок работы с документами и электронными носителями информации, содержащими конфиденциальную информацию

2.1. Учет документов конфиденциального характера.

2.1.1. Конфиденциальная информация, содержащаяся в документах, имеющих обращение в Центре, является служебной информацией конфиденциального характера.

2.1.2. На документах, содержащих конфиденциальную информацию, в необходимых случаях проставляется пометка «Для служебного пользования».

2.1.3. Необходимость проставления пометки «Для служебного пользования» на документах, изданиях и электронных носителях информации, содержащих информацию конфиденциального характера, определяется директором Центра, подписывающим или утверждающим документ. Указанная пометка и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке и титульном листе издания, а также на первой странице сопроводительного письма к таким документам.

2.1.4. Прием и регистрация документов, содержащих информацию конфиденциального характера, осуществляет документовед.

2.1.5. Документы с пометкой «Для служебного пользования»:

- учитываются по экземплярно;
- на обороте последнего листа каждого экземпляра документа должны быть указаны количество отпечатанных экземпляров, фамилия исполнителя и его контактный телефон, дата печатания документа;
- отпечатанные и подписанные документы вместе с черновиками передаются для регистрации;
- черновики уничтожаются с отражением факта уничтожения в учетных формах;
- учитываются, как правило, отдельно от несекретной документации, при незначительном объеме таких документов разрешается вести их учет совместно с другими несекретными документами;
- к регистрационному индексу документа добавляется пометка «ДСП»;
- передаются сотрудникам Центра под расписку;
- пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями;
- размножаются (тиражируются) только с письменного разрешения директора Центра;
- хранятся в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах).

2.1.6. При необходимости направления документов с пометкой «Для служебного пользования» в несколько адресов составляется указатель рассылки, в котором по адресно проставляются номера экземпляров отправляемых документов. Указатель рассылки подписывается исполнителем, готовившим документ.

2.1.7. Исполненные документы с пометкой «Для служебного пользования» группируются в дела, на обложке которых также проставляется пометка «Для служебного пользования».

2.1.8. Уничтожение дел, документов с пометкой «Для служебного пользования», утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

2.1.9. Передача документов и дел с пометкой «Для служебного пользования» от одного сотрудника другому осуществляется с разрешения директора Центра.

2.1.10. При смене сотрудника, ответственного за учет документов с пометкой «Для служебного пользования», составляется акт приема- передачи, который утверждается директором Центра.

2.2. Особенности учета электронных носителей информации, содержащих электронные документы конфиденциального характера.

2.2.1. На съемных электронных носителях информации, содержащих электронные документы конфиденциального характера, проставляется пометка «Для служебного пользования» («ДСП»).

Регистрация отпечатанных с помощью средств вычислительной техники документов, содержащих информацию конфиденциального характера, осуществляется в порядке, определенном для бумажных носителей информации.

Электронные носители информации с конфиденциальной информацией регистрирует документовед. Реквизиты (входящий номер, дата регистрации, пометка «ДСП» и т.д.) проставляются на электронных носителях информации в удобном для просмотра месте.

2.2.2. Электронные носители информации с пометкой «ДСП»:
- регистрируются в Центре с пометкой «ДСП»;
- передаются исполнителям под расписку;
- уничтожаются по акту.

2.2.3. Порядок рассылки, уничтожения, передачи, проверки наличия электронных носителей информации, проведения расследований по фактам утраты электронных носителей информации, снятия пометки «Для служебного пользования» с электронных носителей информации и т.д. является таким же, как и для документов конфиденциального характера.

2.3. Порядок работы с конфиденциальной информацией, представленной в электронном виде.

2.3.1. Хранение, работа и архивирование любых электронных конфиденциальных документов (файлов) должно осуществляться с учётом требования ограничения несанкционированного доступа к ним третьих лиц способами, оговоренными ниже.

2.3.2. Все персональные компьютеры, установленные на рабочих местах сотрудников, должны быть подключены к защищенной корпоративной компьютерной сети Центра (далее – сеть).

2.3.3. Каждый персональный компьютер должен быть оснащён стандартным набором программных средств, принятых для эксплуатации в Центре. Любые изменения в оснащении персонального компьютера,

подключённого к сети, должны быть санкционированы директором Центра, согласованы с ответственным и осуществлены уполномоченными сотрудниками Центра.

2.3.4. Вся конфиденциальная информация, имеющаяся в распоряжении сотрудника, должна храниться и обрабатываться на корпоративном файл-сервере Центра.

2.3.5. Первичный допуск сотрудника к работе на персональном компьютере, включенном в сеть, осуществляется ответственным за информационную безопасность по указанию директора Центра и включает в себя:

-ознакомление сотрудника с настоящим Положением;

-инструктаж по порядку работы с программными средствами, принятыми для эксплуатации в Центре;

-получение сотрудником персонального ключа для шифрования данных;

-получение сотрудником персонального пароля для доступа к ресурсам корпоративного сервера и локальной вычислительной сети;

-получение адреса персонального почтового ящика корпоративной почты.

2.3.6. Сотрудник, допущенный к работе с персональным компьютером, получает доступ:

-к персональному разделу на корпоративном файл-сервере («Личная» папка) для хранения и обработки электронных конфиденциальных документов (файлов) с предоставленной в его распоряжение для выполнения поставленных перед ним задач;

-к персональному почтовому ящику корпоративной почты.

2.3.7. Все электронные конфиденциальные документы (файлы), должны храниться на корпоративном сервере одним из возможных способов:

-в личной папке сотрудника в защищённом на личном ключе виде;

-в личной папке сотрудника в защищённом на личном плюс один или несколько открытых ключей уполномоченных руководства сотрудников виде.

2.3.8. Все новые электронные конфиденциальные документы (файлы) должны создаваться только на файл-сервере в личной папке сотрудника.

2.3.9. Работа с электронными конфиденциальными документами (файлами), допускается только при условии расположения этих документов (файлов) на сервере способами, оговоренными пункте 2.3.7.

2.3.10. В каждый конкретный момент времени в течение рабочего дня загруженными в персональный компьютер сотрудника должны быть только те электронные конфиденциальные документы (файлы), которые имеют непосредственное отношение к тому делу, которым занимается сотрудник в данный момент времени. При этом все другие конфиденциальные документы (файлы), должны находиться на сервере в виде согласно пункту 2.3.7.

2.3.11. Загрузка (открытие), сверх действительно необходимого количества, электронных конфиденциальных документов (файлов) на персональных компьютерах сотрудников запрещается.

2.3.12. В течение рабочего дня ставшие ненужными в текущей работе (отработанные) электронные конфиденциальные документы (файлы) подлежат незамедлительному закрытию (сохранению на файл-сервер).

2.3.13. С целью недопущения переполнения сетевых дисков, выявленные в течение дня ненужные файлы (старые версии файлов и т.д.) подлежат безусловному незамедлительному уничтожению.

2.3.14. Уничтожение электронных конфиденциальных документов (файлов) с сетевых дисков корпоративного файл-сервера осуществляется стандартными средствами операционной системы – команда «Удалить» контекстного меню. Уничтожение электронных конфиденциальных документов (файлов) с любых иных носителей должно осуществляться только с помощью утилиты Wipe специально предназначенной для уничтожения файлов без возможности их последующего восстановления.

2.3.15. Обмен электронными конфиденциальными документами (файлами) между сотрудниками, находящимися в офисе, осуществляется в зашифрованном виде одним из способов:

-используя сервис программы ICQ;

-используя сервис корпоративной почты.

2.3.16. Обмен электронными конфиденциальными документами (файлами) между сотрудниками, находящимися вне Центра осуществляется путем обмена зашифрованной почтой через корпоративные почтовые ящики сотрудников.

2.3.17. В случае прихода (ожидания) посетителя к сотруднику, в персональный компьютер этого сотрудника могут быть загружены только те электронные конфиденциальные документы (файлы), относящиеся к делу этого посетителя. Загружать в персональный компьютер и/или работать с электронными конфиденциальными документами (файлами), не относящимися к делу присутствующего посетителя, запрещается.

2.3.18. Сотруднику, работающему с электронными конфиденциальными документами (файлами) категорически запрещается:

- оставлять персональный компьютер на время более 5 мин. с разрешённым доступом к личной папке;

- сообщать, кому бы то ни было, свой персональный пароль доступа в закрытую корпоративную компьютерную сеть Центра;

- сообщать, кому бы то ни было, пароль доступа к своему персональному ключу PGP;

- оставлять посетителя в кабинете одного при включенном в защищенную корпоративную сеть компьютере;

- осуществлять хранение/обработку личных файлов (данных, не имеющих отношения к выполнению функциональных обязанностей, а

именно: файлы mp3, игры, картинки, личные фотографии и т.д.) на сетевых дисках корпоративного сервера;

- использовать съёмные носители (дискеты, ZIP диски, магнитооптика и т.д.) для обмена между сотрудниками и хранения электронных конфиденциальных документов (файлов);

- самовольно, без согласования с ответственным, изменять аппаратную конфигурацию и настройки программного обеспечения персональных компьютеров, подключенных к сети.

## 3. Обязанности и ответственность сотрудников по защите конфиденциальной информации

3.1. В круг лиц, имеющих доступ к конфиденциальной информации, входят: директор Центра, его заместители, классные руководители, воспитатели, старшие воспитатели, специалисты по кадрам, документоведы, делопроизводители, другие работники по распоряжению директора Центра.

3.2. Директор Центра:

3.2.1. Назначает ответственного за организацию и обеспечение защиты информации из числа сотрудников МКОУ «Быковская СШ №2».

3.2.2. Утверждает:

- состав комиссии по организации работ по защите информации,

- меры и состав средств системы защиты информации для обеспечения защиты конфиденциальной информации,

- перечень сведений конфиденциального характера.

3.2.3. Осуществляет контроль работы ответственного за организацию и обеспечение защиты информации.

3.2.4. Создает в канцелярии Центра условия, ограничивающие доступ к конфиденциальной информации третьих лиц и несанкционированное разглашение конфиденциальной информации, в том числе устанавливает технические средства защиты от несанкционированного доступа к информации (сейфы и металлические ящики для хранения документов и пр.).

3.3. Ответственный за организацию и обеспечение защиты информации:

3.3.1. Разрабатывает организационно распорядительные документы по вопросам защиты информации при ее обработке с помощью информационных систем.

3.3.2. Контролирует исполнение приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности информации.

3.3.3. Обеспечивает защиту информации, циркулирующей на объектах информатизации.

3.3.4. Проводит инструктаж пользователей информационными системами.

3.3.5. Присутствует (участвует) в работах по внесению изменений в аппаратно-программную конфигурацию информационных систем.

3.3.5. Принимает меры по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших допуск к информационным системам, к конфиденциальной информации.

3.3.6. Дает обязательные для исполнения указания по работе с информационными системами, с конфиденциальной информацией.

3.3.7. Требует устранения выявленных нарушений и недостатков.

3.3.8. Требует от работников представления письменных объяснений по фактам нарушения режима конфиденциальности.

3.3.9. Готовит в установленные сроки необходимую отчетную документацию о состоянии работы информационных систем, по защите конфиденциальной информации.

3.3.10. Доводит до сведения директора Центра информацию:

- об имеющихся недостатках и выявленных нарушениях требований нормативных и распорядительных документов по защите информации;

- о выявлении попыток несанкционированного доступа к конфиденциальной информации или попыток хищения, копирования, изменения конфиденциальной информации.

3.3.11. Принимает меры пресечения попыток несанкционированного доступа к конфиденциальной информации или попыток хищения, копирования, изменения конфиденциальной информации.

3.3.12. Проводит с сотрудниками, ответственными за обработку персональных данных и владеющими конфиденциальной информацией, инструктаж по соблюдению режима конфиденциальной информации. Данные о проведенном инструктаже фиксируются в специальном журнале.

3.4. При приеме на работу сотрудники Центра предупреждаются об ответственности за разглашение конфиденциальной информации или служебной информации, ставшие им известными в связи с выполнением своих должностных обязанностей.

3.5. Сотрудники Центра, допущенные к конфиденциальной информации, должны:

- хранить конфиденциальную информацию, в том числе не сообщать конфиденциальные сведения друзьям и членам своей семьи. О ставших им известной утечке сведений, составляющих конфиденциальную информацию, а также об утрате документов с грифом «ДСП», немедленно сообщать ответственному за информационную безопасность или директору Центра;

- предъявлять для проверки все числящиеся за ними материалы, содержащие конфиденциальную информацию, а в случае нарушения установленных правил работы с ними представлять соответствующие объяснения в устном и письменном виде;

- знакомиться только с теми документами и выполнять только те работы, к которым они допущены в соответствии с функциональными обязанностями и с дополнительными задачами, возложенными на них администрацией Центра;

- соблюдать правила пользования и сохранности документов, имеющих гриф «ДСП», не допускать их необоснованной рассылки;

- исключать возможность ознакомления с конфиденциальной информацией, посторонних лиц, включая и сотрудников Центра, не имеющих к указанным материалам прямого отношения;

- при ведении деловых переговоров с представителями сторонних организаций или частными лицами ограничиваться выдачей минимальной информации, действительно необходимой для их успешного завершения; - при временном убытии (в отпуск, командировку, на учебу, лечение и т.д.) проверять наличие числящихся за ним конфиденциальных документов. Документы, которые подлежат исполнению или могут потребоваться в работе, передавать другому сотруднику по указанию руководства организации или руководства структурного подразделения. При прекращении трудовых или иных договорных отношений с Организацией, сотрудник обязан сдать все числящиеся за ним конфиденциальные документы;

- исключить использование конфиденциальной информации в свою личную пользу, а также исключить деятельность, которая может быть использована в ущерб Центру.

3.6. Сотрудник, работающий с электронными конфиденциальными документами (файлами) обязан:

- выполнять требования ответственного в рамках установленного регламента эксплуатации сети и требований настоящего Положения (технический перерыв, устранение выявленных нарушений хранения/обработки данных, профилактические работы на оборудовании сети). Несоблюдение требований настоящего пункта может привести к необратимой потере данных, ответственность за которую возлагается на самих сотрудников;

- при убытии в отпуск/командировку предоставить имеющиеся у него конфиденциальные электронные документы (файлы), которые могут понадобиться в его отсутствие (определяется директором Центра), в распоряжение уполномоченного руководителем сотрудника в зашифрованном на открытом ключе этого сотрудника виде;

- ежедневно в конце рабочего дня производить «зачистку» локального диска своего персонального компьютера путём запуска соответствующей процедуры (ярлык «До свидания!» на рабочем столе Windows);

- еженедельно производить ревизию своей личной папки, размещённой на корпоративном файл-сервере, с целью выявления и уничтожения конфиденциальных электронных документов (файлов) ставших ненужными.

3.7. Сотрудники Центра несут персональную ответственность за разглашение конфиденциальной информации.

За разглашение конфиденциальной информации, а также нарушение порядка обращения с электронными носителями информации и документами, содержащими такую информацию, за нарушение режима

защиты, обработки и порядка использования этой информации сотрудник может быть привлечен к ответственности, предусмотренной действующим законодательством.

Ответственность за разглашение конфиденциальной информации, и утрату документов, содержащих такие сведения устанавливается в соответствии с Уголовным кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Кодексом Российской Федерации об административных правонарушениях, Трудовым кодексом Российской Федерации и иным действующим законодательством.

3.8. Разглашением конфиденциальной информации следует считать следующие действия сотрудника:

3.8.1. Доведение до сведения неуполномоченных лиц в устной, письменной, электронной или иной форме конфиденциальную информацию. Указанный факт может наступить в результате умысла сотрудника или по неосторожности, включая халатное отношение к своим обязанностям;

3.8.2. Использование конфиденциальной информации в процессе выполнения работы для другого учреждения и организации или по заданию физического лица;

3.8.3. Использование конфиденциальной информации в научной и педагогической деятельности;

3.8.4. Использование конфиденциальной информации в личных целях, не связанных с выполнением должностных обязанностей в Центре;

3.8.5. Использование конфиденциальной информации в ходе публичных выступлений, интервью и т.п.;

3.8.6. Иные действия сотрудника, в результате которых конфиденциальная информация, стала известна неуполномоченным лицам.

3.9. Не считаются разглашением конфиденциальной информации действия сотрудника, указанные в пункте 3.8. настоящего Положения, совершенные им в порядке и в случаях, предусмотренных законодательством Российской Федерации, во исполнение нормативных актов Центра или договоров (соглашений) Центра с иными организациями или физическими лицами. Не считаются разглашением конфиденциальной информации действия сотрудника, совершенные им при наличии письменного разрешения или иного указания директора Центра.

3.10. По фактам разглашения конфиденциальной информации, директором Центра назначается служебное разбирательство.

3.11. Если действиями (бездействием) сотрудника, связанными с нарушением правил обращения с конфиденциальной информацией, причинен материальный ущерб, возмещение ущерба производится в порядке, предусмотренном законодательством Российской Федерации.

3.12. Директор Центра, принявший решение об отнесении информации к категории конфиденциального характера, несет персональную ответственность за обоснованность принятого решения.

## 4. Порядок обеспечения сохранности документов и дел (архивов), содержащих конфиденциальную информацию

4.1. Все документы, и дела (архивы) с документами, имеющими гриф «ДСП», должны храниться в помещениях в надежно запираемых и опечатываемых сейфах (металлических шкафах). Помещения должны отвечать требованиям внутри объектного режима, обеспечивающего физическую сохранность находящейся в них документации.

4.2. Дела (архивы) с документами, имеющими гриф «ДСП», выдаются документоведом под роспись в регистрационном журнале и подлежат возврату сотрудниками в тот же день. При необходимости, с разрешения директора Центра, они могут находиться у сотрудника в течение срока, необходимого для выполнения задания, при условии полного обеспечения их сохранности и соблюдения правил хранения.

4.3. С документами (электронными и бумажными) с грифом «ДСП» разрешается работать только в помещениях Центра. Для работы вне помещений необходимо разрешение директора Центра.

4.4. Во время перерывов в работе, связанных с выходом из своего офисного помещения, запрещается оставлять конфиденциальные документы на столах, в незапертых ящиках столов. В случае нахождения в офисном помещении посетителей или иных лиц, не имеющих допуск к конфиденциальным бумажным документам, все конфиденциальные документы должны быть убраны.

4.5. Изъятия из дел (архивов) или перемещение бумажных документов с грифом «ДСП» из одного дела (архива) в другое без санкции директора Центра запрещается.

4.6. Смена секретарей, ответственных за учет и хранение документов, дел (архивов) с грифом «ДСП», оформляется приказом директора Центра. При этом составляется акт приема-передачи этих материалов, утверждаемый директором Центра.

## 5. Порядок допуска к конфиденциальной информации

5.1. Допуск сотрудников к конфиденциальной информации осуществляется директором Центра и оформляется приказом.

5.2. Администрация Центра обеспечивает систематический контроль за допуском к конфиденциальной информации только тех лиц, которым они необходимы для выполнения функциональных обязанностей.

5.3. К конфиденциальной информации допускаются лица, личные и деловые качества которых обеспечивают их способность хранить конфиденциальную информацию, и только после оформления письменного обязательства по сохранению конфиденциальной информации.

5.4. Допуск сотрудников к работе с делами (архивами), в которых хранится конфиденциальная информация, осуществляется согласно оформленному на внутренней стороне обложки дела (архива) или на отдельном листе списку допущенных сотрудников за подписью директора

Центра, а к документам - в соответствии с указаниями, содержащимися в резолюциях директора Центра.

5.5. Представители сторонних организаций и частные лица могут быть допущены к ознакомлению и работе с документами и делами (архивами) с грифом «ДСП» только с разрешения директора Центра.

## 6. Контроль выполнения требований внутри объектового режима при работе с конфиденциальной информацией

6.1. Под внутри объектовым режимом при работе с конфиденциальной информацией подразумевается соблюдение условий работы, исключающих возможность утечки информации о конфиденциальных сведениях.

6.2. Контроль за соблюдением указанного режима осуществляется в целях изучения и оценки состояния сохранности конфиденциальной информации, выявления и установления причин недостатков, и выработки предложений по их устранению.

6.3. Контроль обеспечения режима при работе с конфиденциальной информацией осуществляют директор Центра, ответственный за информационную безопасность путем текущих и внеплановых проверок.

6.4. При проведении проверок создается комиссия, которая комплектуется из сотрудников Центра организации в составе не менее двух человек, допущенных к работе с материалами, имеющими гриф «ДСП».

6.5. Участие в проверке не должно приводить к необоснованному увеличению осведомленности в этих сведениях, а также затруднять работу сотрудников Центра.

6.6. Плановые проверки проводятся не реже одного раза в год на основании приказа директора Центра.

6.7. Внеплановые проверки проводятся при наличии признаков утечки конфиденциальной информации или по иной необходимости на основании распоряжения директора Центра.

6.8. Проверяющие имеют право знакомиться со всеми документами и иными материалами, имеющими отношение к проверяемым вопросам, а также проводить беседы, консультироваться со специалистами и исполнителями, требовать представления письменных объяснений, справок и отчетов по всем вопросам, входящим в компетенцию комиссии.

6.9. По результатам проверок составляется акт с отражением в нем наличия документов, состояния работы с материалами, имеющими гриф «ДСП», выявленных недостатков и предложений по их устранению. Акт подписывается членами комиссии и утверждается директором Центра.

6.10. При выявлении случаев утраты документов или разглашения конфиденциальной информации ставится в известность директор Центра и (или) ответственный за информационную безопасность. Для расследования указанных случаев приказом директора Центра создается комиссия, которая определяет соответствие содержания утраченного документа проставленному грифу «ДСП» и выявляет обстоятельства утраты

(разглашения), а также предложения по минимизации потерь, связанных утратой документа или разглашением конфиденциальной информации. По результатам работы комиссии составляется акт.

Приложение
к Положению о защите
конфиденциальной информации

Сводный перечень сведений конфиденциального характера

| № п/п | Содержание сведений | Основания для включения |
|---|---|---|
| 1. | Сведения о частной жизни, переписке, телефонных переговорах, почтовых, телеграфных и иных сообщениях, личной и семейной тайне | Ст.ст. 23, 24 Конституции Российской Федерации |
| 2. | Информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (персональные данные) | Ст. 86 ТК РФ |
| 3. | Сведения, содержащиеся в записях актов о рождении, о смерти, о заключении брака, о расторжении брака, об установлении отцовства, о перемене имени, а также сведения о тайне усыновления (удочерения), за исключением сведений, разглашение которых осуществлено по воле усыновителя | п. 7 ст. 13.1 Федерального закона от 15.11.1997 №143-ФЗ «Об актах гражданского состояния» |
| 4. | Сведения (персональные данные), относящиеся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) | Ст. 7 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» |
| 5. | Сведения о доходах, об имуществе и обязательствах имущественного характера | Ст. 8 Федерального закона от 25.12.2008 №273-ФЗ «О противодействии коррупции» |
| 6. | Сведения, получаемые при осуществлении закупок товаров, работ, услуг для обеспечения муниципальных нужд | Ст. 51 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» |
| 7. | Сведения, содержащиеся в индивидуальных лицевых счетах застрахованных лиц: страховой номер; фамилия, имя и отчество; | Ст. 17 Федерального закона 01.04.1996 № 27-ФЗ «Об |

| | | |
|---|---|---|
| | фамилия, которая была у застрахованного лица при рождении; дата рождения; место рождения; пол; адрес постоянного места жительства; серия и номер паспорта или удостоверения личности, дата выдачи указанных документов, наименование выдавшего их органа; гражданство; номер телефона; периоды трудовой и иной общественно-полезной деятельности, включаемые в общий стаж для назначения трудовой пенсии, а также специальный стаж, связанный с особыми условиями труда, работой в районах Крайнего Севера и приравненных к ним местностях, выслугой лет. Работой на территориях, подвергшихся радиоактивному загрязнению; заработная плата или доход (за каждый месяц страхового), на которые начислены страховые взносы в Пенсионный фонд Российской Федерации в соответствии с законодательством Российской Федерации;<br>сумма заработка (за каждый месяц страхового стажа), который учитывается при назначении трудовой пенсии; сумма начисленных данному застрахованному лицу страховых взносов (за каждый месяц страхового стажа), включая страховые взносы за счет работодателя и страховые взносы самого застрахованного лица; периоды выплаты пособия по безработице; периоды военной службы и другой приравненной к ней службы, включаемые в общий трудовой стаж; сведения о назначении (перерасчете), индексации | индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» |
| 8. | Сведения, содержащиеся в регистрах бухгалтерского учета, внутренней бухгалтерской отчетности организаций | Ст. 10 Федерального закона от 06.12.2011 №402-ФЗ «О бухгалтерском учете» |
| 9. | Сведения, представляемые в Государственную статистическую отчетность по конкретному хозяйствующему субъекту | Перечень служебной информации ограниченного распространения, утвержденный |

| | | |
|---|---|---|
| | | Председателем Госкомстата России 14.02.2002 |
| 10. | Сведения об охране МБОУ ЦО № 44, пропускном и внутриобъектовом режиме, системе сигнализации, о наличии средств контроля и управления доступом | Письмо Министерства образования и науки Российской Федерации от 30.08.2005 № 03-1572 «Об обеспечении безопасности в образовательных учреждениях» |
| 12. | Сведения о специальных средствах, технических приемах, тактике осуществления мероприятий по борьбе с терроризмом, а также о составе их участников | Ст. 2 Федерального закона от 06.03.2006 №35-ФЗ «О противодействии терроризму» |