

Согласовано:

Председатель Профсоюзного комитета
Муниципального бюджетного
образовательного учреждения
дополнительного образования «Центр
развития образования» Питкярантского
муниципального округа (МБОУ ДО
«ЦРО»)



Бушковская Г.И.

«17» февраля 2026 года

Утверждаю:

Директор Муниципального бюджетного
образовательного учреждения
дополнительного образования «Центр
развития образования» Питкярантского
муниципального округа (МБОУ ДО
«ЦРО»)



Дожидаева Т.Г.

«17» февраля 2026 года

Приказом № 10-ОД от 17.02.2026 г.

**Положение
о конфиденциальной информации
Муниципальное бюджетное образовательное учреждение дополнительного образования
«Центр развития образования» Питкярантского муниципального округа**

I. Назначение

1.1. Настоящее Положение о конфиденциальной информации МБОУ ДО «ЦРО» (далее – Положение) определяет перечень конфиденциальной информации, обрабатываемой в МБОУ ДО «ЦРО» (далее – Учреждение), регламентирует оборот в Учреждении документов, содержащих информацию ограниченного доступа, не относящуюся к государственной тайне, в соответствии с требованиями и принципами, установленными действующим законодательством.

1.2. Настоящее Положение определяет общие требования, предъявляемые к регистрации, учёту, оформлению, тиражированию, хранению, использованию, уничтожению, перерегистрации конфиденциальных документов и других материальных носителей информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, а также устанавливает порядок доступа к указанной информации.

II. Область применения

2.1. Выполнение требований Положения является обязательным для сотрудников Учреждения, сотрудников иных органов и организаций, а также сотрудников надзорно-контрольных органов, получивших в установленном порядке доступ к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности.

2.2. Настоящее Положение используется совместно с Порядком обращения с конфиденциальной информацией и средствами криптографической защиты в МБОУ ДО «ЦРО» утвержденным приказом № 10-ОД от 17.02.2026 г.

III. Нормативные ссылки

3.1. Настоящее Положение разработано в соответствии со следующими нормативными правовыми актами:

- статьями 23 и 24 Конституции Российской Федерации;
- 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»;

- ст.6 Федерального закона от 28.12.2013 № 442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации»;
- главой 14 Трудового кодекса Российской Федерации;
- Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» (с изменениями на 13 июля 2015 года);
- Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- ГОСТ Р 7.0.97-2016 Система стандартов по информации, библиотечному и издательскому делу (СИБИД). Организационно-распорядительная документация. Требования к оформлению документов (с Изменением N 1);
- ГОСТ Р 7.0.8-2013 СИБИД. Делопроизводство и архивное дело. Термины и определения;
- ГОСТ Р ИСО 15489-1-2019. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы" (утв. Приказом Росстандарта от 26.03.2019 N 101-ст);
- ПРИКАЗ от 20 декабря 2019 года N 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»;
- Приказ ФСТЭК России от 11.02.2013 N 17 (ред. от 28.05.2019) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (Зарегистрировано в Минюсте России 31.05.2013 N 28608) (с изм. и доп., вступ. в силу с 01.01.2021)

IV. Термины, обозначения и сокращения

- 4.1 В настоящем Положении используются следующие термины, обозначения и сокращения:
- 4.2 Конфиденциальная информация - любые сведения, составляющие служебную, коммерческую тайну, включая персональные данные сотрудников и обучающихся.
- 4.3 Владелец конфиденциальной информации - лицо, которое владеет информацией, составляющей конфиденциальную информацию, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим конфиденциальной информации. Владелец информации, составляющей конфиденциальную информацию, является образовательное учреждение.
- 4.4 Информация - сведения (сообщения, данные) независимо от формы их представления.
- 4.4.1 Служебная тайна - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании, и в отношении которой владельцем такой информации введен режим коммерческой тайны. Информация может быть отнесена к служебной тайне в том, случае, если она получена, разработана в процессе осуществления трудовых правоотношений и не влечет (не может повлечь) получения прибыли владельцем такой информации. Служебную тайну организации составляют любые сведения, в том числе сведения, содержащиеся в служебной переписке, телефонных переговорах, почтовых отправлениях, телеграфных и иных сообщениях, передаваемых по сетям электрической и почтовой связи, которые стали известны работнику организации в связи с исполнением им возложенных на него трудовых обязанностей. К служебной тайне не относится информация, разглашенная образовательным учреждением

самостоятельно или с её согласия, а также иная информация, ограничения доступа к которой не допускаются в соответствии с законодательством РФ.

4.4.2 Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду; научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны. Информация может быть отнесена к коммерческой тайне в том, случае, если она получена, разработана в процессе осуществления трудовых правоотношений, либо в результате гражданско-правовых отношений, влекущая или могущая повлечь получение прибыли обладателем такой информации.

4.4.3 Врачебная тайна - информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении.

4.4.4 Персональные данные сотрудника, учащегося - любая информация, относящаяся к сотруднику, учащемуся, как субъекту персональных данных, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, сведения о фактах, событиях и обстоятельствах жизни сотрудника, воспитанника, позволяющие идентифицировать его личность.

4.4.5 Доступ к конфиденциальной информации - ознакомление определенных лиц с информацией, составляющей тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

4.4.6 Передача конфиденциальной информации - передача информации, составляющей тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

4.4.7 Предоставление информации, составляющей тайну, - передача информации, составляющей тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

4.4.8 Разглашение конфиденциальной информации - действие или бездействие, в результате которых информация, составляющая тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

V. Конфиденциальная информация и ее отношение к различным видам тайн

5.1 Частью 3 статьи 5 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями на 30 декабря 2020 года)

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

5.2 Перечнем сведений конфиденциального характера, определено, что к конфиденциальной информации относятся:

– сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

– сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну;

– служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

– сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

– сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

– сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них;

– сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии.

5.3 Таким образом, все виды тайн, не являющиеся информацией, относимой к государственной тайне, являются частным проявлением более широкого понятия «конфиденциальная информация» или «информация, в отношении которой установлено требование об обеспечении ее конфиденциальности».

5.4 Одна и та же по содержанию информация в зависимости от обстоятельств может находиться под защитой как одного, так и нескольких правовых режимов защиты. Кроме того, одна и та же информация в зависимости от отношения к ее обладателю может выступать как тайны различного вида. Например: персональные данные являются одним из видов информации, в отношении которой установлено требование об обеспечении ее конфиденциальности. При этом, по отношению к субъекту персональных данных эта информация может являться личной тайной, а по отношению к государственному или муниципальному служащему, обрабатывающему персональные данные иных субъектов на законном основании, эта информация выступает в виде служебной тайны.

5.5 В организациях и учреждениях в соответствии с Перечнем сведений конфиденциального характера, принят гриф ограниченного доступа Конфиденциально.

5.6 Учреждение, являясь подведомственным Министерству Образования и Спорта учреждением, использует гриф ограниченного доступа «Конфиденциально».

Из сказанного выше следует, что:

5.6.1 при поступлении в Учреждение из органов государственной власти, местного самоуправления, других организаций или учреждений, из ЦБ ПМР, от руководителя учреждения документов, содержащих информацию ограниченного доступа, не относящуюся к сведениям, составляющим государственную тайну, и имеющих гриф конфиденциальности «Конфиденциально», «Для служебного пользования», для «Внутреннего использования», «Только для отдела ...» и др., регистрация и учет поступивших документов должен проводиться в соответствии с настоящим Положением;

5.6.2 термины: «информация, в отношении которой установлено требование об обеспечении ее конфиденциальности»¹, «конфиденциальная информация»², «информации

ограниченного доступа, не содержащая сведения, составляющие государственную тайну»³ определяют одно и то же понятие;

5.6.3 термины «конфиденциальная информация» и «служебная тайна» в отношении информации ограниченного доступа, не относящейся к государственной тайне и находящейся в распоряжении сотрудников Учреждения на законном основании, определяют одно и то же понятие, и не является служебной тайной как таковой.

VI. Режим ограниченного доступа к конфиденциальной информации

6.1 Режим ограниченного доступа к конфиденциальной информации Учреждения предполагает:

6.1.1 утверждение Перечня сведений конфиденциального характера Учреждения;

6.1.2 установление единого порядка допуска к конфиденциальной информации;

6.1.3 установление единого порядка обращения в Учреждении конфиденциальных документов (создание, регистрация, прием, отправление, хранение, уничтожение);

6.1.4 установление разрешительной системы допуска к информационным ресурсам информационных систем

6.1.5 утверждение Правил об использовании электронной почты (Приложение 2 к настоящему Положению).

VII. Организация допуска к конфиденциальной информации

7.1 Учёт лиц, получивших доступ к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, и лиц, которым такая информация была предоставлена или передана

7.1.1В Учреждении ведется учет:

- сотрудников Учреждения, получивших доступ к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, а также информации, в отношении которой они получили доступ в соответствии с нижеизложенным перечнем должностей учреждения, допущенных к работе с конфиденциальной информацией:

Перечень должностей сотрудников

- директор МБОУ ДО «ЦРО»
- специалист ответственный за кадровую работу
- сотрудник ответственный за ОТ и ПБ;
- сотрудники Централизованной бухгалтерии ПМО;
- сотрудники, предоставившие предприятию свои персональные данные;
- непосредственные руководители отделов;
- специалисты.

- должностных лиц органов государственной власти, иных государственных органов, получивших доступ к находящейся в ведении Учреждения информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, в период проведения ими проверок в Журнале проверок;

- на специалиста (по кадровой работе) возлагаются функции по организации и ведению конфиденциального делопроизводства.

7.2 Порядок допуска к конфиденциальной информации сотрудников Учреждения

7.2.1 Допуск сотрудников Учреждения к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, осуществляется на основании:

7.2.1.1 наличия должности сотрудника, допускаемого к конфиденциальной информации, в Перечне должностей сотрудников, замещение которых предусматривает допуск сотрудника к конфиденциальной информации Учреждения.

7.2.1.2 изучения сотрудником, допускаемым к указанной информации, требований настоящего Положения и его росписи в листах (журнале) ознакомления;

7.2.1.3 получение от сотрудника не указанного в Перечне, но допускаемого к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности «Обязательства о неразглашении конфиденциальной информации Учреждения» (Приложение №1 к настоящему Положению).

7.2.2 Руководители структурных подразделений Учреждения осуществляют контроль допуска подчиненных сотрудников к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности.

7.2.3 Процедура допуска к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности:

7.2.3.1 Специалист (ответственный за кадровое делопроизводство):

7.2.3.1.1 организует изучение положений и требований сотрудниками Учреждения, допускаемыми к конфиденциальной информации, под подпись в листах (журнале) ознакомления с настоящим Положением.

7.2.3.1.2 обеспечивает хранение листов (журнала) ознакомления с настоящим Положением;

7.2.3.1.3 принимает от сотрудников Учреждения Обязательства о неразглашении конфиденциальной информации, не содержащей сведений, составляющих государственную тайну (Приложение №1 к настоящему Положению).

VIII. Порядок обращения в Учреждении конфиденциальных документов

8.1 Порядок подготовки, оформления документов, учета и хранения материальных носителей конфиденциальной информации

8.1.1 Если форма документа утверждена нормативным актом органа государственной власти или местного самоуправления и при этом указанная форма документа не предусматривает проставления грифа ограничения доступа (конфиденциальности), но сам документ содержит сведения, отнесенные к конфиденциальной информации в соответствии с законодательством или Перечнем сведений конфиденциального характера Учреждения, то гриф конфиденциальности на указанном документе не ставится, а хранение, пересылка и другие действия с указанным документом осуществляются в соответствии с настоящим Положением.

Например: Форма трудовой книжки утверждена Постановлением Правительства РФ от 16.04.2003 №225 «О трудовых книжках» (вместе с «Правилами ведения и хранения трудовых книжек, изготовления бланков трудовой книжки и обеспечения ими работодателей»). Данная форма не содержит грифа конфиденциальности, но при заполнении трудовой книжки в нее вносятся персональные данные, отнесенные к конфиденциальной информации в соответствии с Указом Президента РФ от 06.03.1997 №188 «Об утверждении Перечня сведений конфиденциального характера» Хранение трудовой книжки должно производиться в соответствии с правилами хранения материальных носителей конфиденциальной информации.

8.1.2 Сотрудник Учреждения, ответственный за ведение делопроизводства или хранение конфиденциальных документов, несет персональную ответственность за их сохранность и выдачу только лицам, допущенным к конфиденциальной информации в порядке раздела VII настоящего Положения. Допуск к конфиденциальной информации иных лиц возможен только после письменного указания директора учреждения.

8.1.3 Места и сроки хранения конфиденциальных документов, предусмотрены Приложением к Положению. Хранение конфиденциальных и неконфиденциальных документов должно быть раздельным. Возможно совместное хранение в конфиденциальном деле конфиденциальных и неконфиденциальных документов, объединенных общей темой. Ознакомление лица, не имеющего допуска к конфиденциальной информации, с

неконфиденциальным документом, хранящимся в конфиденциальном деле, должен исключить возможность его ознакомления с иными конфиденциальными документами указанного дела.

8.1.4 Хранение носителей конфиденциальной информации осуществляется в местах, исключающих несанкционированный доступ к ним посторонних лиц. При этом:

8.1.4.1 трудовые книжки хранятся в сейфах (металлических шкафах) как бланки строгой отчетности⁴;

8.1.4.2 съемные носители конфиденциальной информации в незашифрованном с использованием средств криптографической защиты информации (далее-СКЗИ) виде хранятся в сейфах (металлических шкафах)

8.1.4.3 дубликаты ключей от хранилищ со СКЗИ хранятся у директора учреждения в соответствии.

8.1.5 Снятие ограничения доступа к конфиденциальным документам производится по акту постоянно действующей экспертной комиссии, утвержденному директором Учреждения.

8.2 Порядок предоставления конфиденциальной информации Учреждения третьим лицам

8.2.1 По общему правилу предоставление конфиденциальной информации Учреждения третьим лицам возможно только на законном основании по указанию директора Учреждения, несущего персональную ответственность за принятое решение.

8.2.2 Предоставление персональных данных как вида конфиденциальной информации имеет ряд особенностей:

8.2.2.1 сотрудники и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

8.2.2.2 В соответствии с федеральным законодательством Учреждение обязано предоставлять персональные данные субъектов следующим органам (организациям) или их должностным лицам:

8.2.2.2.1 по мотивированному запросу прокурора, руководителя следственного органа, следователя, органа дознания и дознавателя, предъявленному в пределах их полномочий, установленных Уголовно-процессуальным кодексом Российской Федерации";

8.2.2.2.2 военным комиссариатам – сведения о воинском учете сотрудников (категория запаса, воинское звание, состав (профиль), полное кодовое обозначение ВУС, категория годности к военной службе, наименование комиссариата по месту жительства, воинский учет (общий, специальный);

8.2.2.2.3 налоговым органам – фамилия, имя, отчество, дата и место рождения сотрудника; его оклад; произведенные сотруднику начисления и выплаты, данные о заработной плате, номер лицевого счета в банке; табельный номер, суммарный доход с начала года;

8.2.2.2.4 территориальным органам Пенсионного фонда РФ – номер страхового свидетельства государственного пенсионного страхования сотрудника, стаж для расчета страховой части пенсионных накоплений сотруднику;

8.2.2.2.5 участникам межведомственного взаимодействия в пределах их полномочий, установленных действующим законодательством;

8.2.2.2.6 иным органам, организациям и физическим лицам в соответствии с действующим законодательством.

8.3 Уничтожение документов, содержащих конфиденциальную информацию

8.3.1 Уничтожение документов, содержащих конфиденциальную информацию производится по акту.

⁴ См. п.42 Правил ведения и хранения трудовых книжек, изготовления бланков трудовой книжки и обеспечения ими работодателей, утвержденных Постановлением Правительства РФ от 16.04.2003 №225.

8.3.2 Отобранные к уничтожению документы измельчаются механическим способом до степени, исключающей возможность прочтения текста, или сжигаются в печи до золы.

8.3.3 Хранение конфиденциальной информации в необезличенном виде на магнитных носителях не допускается.

8.3.4 В целях гарантированного уничтожения файлов и затирания остаточной информации на магнитном носителе либо уничтожения носителей механическим способом привлекается сторонний специалист.

8.3.5 Факт уничтожения конфиденциальных материалов оформляется соответствующим актом, утверждаемым директором Учреждения.

8.3.6 По факту утраты конфиденциальных документов, дел и других материалов или разглашения сведений, содержащихся в этих материалах, проводится служебная проверка и составляется заключение служебной проверки, которая утверждается директором Учреждения⁵.

IX. Ответственность и полномочия персонала

Ответственность персонала

9.1 Ответственность за несоблюдение требований, установленных настоящим Положением, несут:

- сотрудники, ответственные за организацию обработки персональных данных в Учреждении, за осуществление контроля организации допуска сотрудников Учреждения и сотрудников иных органов и организаций к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, а также за контроль поддержания установленного уровня защиты конфиденциальной информации, за организацию допуска сотрудников Учреждения к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности;
- сотрудник ответственный за организацию конфиденциального делопроизводства в Учреждении и организацию допуска сотрудников иных органов и организаций к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности;
- ответственный за защиту персональных данных в информационной системе персональных данных за осуществление защиты конфиденциальной информации в информационных системах;
- администратор локальной сети за поддержание установленного уровня защищенности информационных систем, обрабатывающих конфиденциальную информацию;
- директор и руководители структурных подразделений Учреждения за контроль выполнения требований настоящего Положения в Учреждении и вверенных им подразделениях;
- сотрудники Учреждения и иные лица, допущенные в установленном порядке к информации, в отношении которой установлены требования об обеспечении ее конфиденциальности, за неисполнение требований настоящего Положения в части, их касающейся.

⁵ Исполняется в соответствии с:

- п. 7 Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001. № 152 (Бюллетень нормативных актов федеральных органов исполнительной власти, 2001. № 34);
- п. 2.3. и п. 3.24. «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622;

9.2 Руководитель, принявший решение, влияющее на защищенность информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, несет персональную ответственность за принятое решение.

9.3 Лица, указанные в п.9.1.1 настоящего Положения, за нарушение требований действующего законодательства и настоящего Положения несут уголовную, гражданскую, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.

9.4 Полномочия персонала

9.4.1 Сотрудники Учреждения имеют право выходить с предложениями к руководству Учреждения по вопросам защиты конфиденциальной информации. Изменения в настоящее Положение вносятся приказом Учреждения после обязательного согласования вносимых изменений с Профсоюзом.

Директор
МБОУ ДО «ЦРО»



Дожидаева Т.Г.

**Перечень
конфиденциальной информации МБОУ ДО «ЦРО» ПМО**

1. Сводный перечень сведений конфиденциального характера (далее именуется "Перечень") составлен на основании нормативных правовых актов Российской Федерации, относящих сведения к категории конфиденциальных.
2. Конфиденциальность сведений, содержащихся в работах, документах и изданиях, определяется по настоящему развернутому Перечню, составленному в соответствии с действующим законодательством.
3. Конфиденциальность документов, составленных на основании материалов, поступивших из других организаций, определяется степенью конфиденциальности сведений, содержащихся в этих материалах.

1. Персональные данные учащегося:

- ✓ ФИО;
- ✓ пол;
- ✓ дата рождения;
- ✓ адрес регистрации;
- ✓ фотография;
- ✓ адрес фактического проживания;
- ✓ контактный телефон;
- ✓ данные свидетельства о рождении;
- ✓ иные данные необходимые для организации педагогического процесса
- ✓ сведения о состоянии здоровья и иные медицинские сведения.

2. Персональные данные сотрудника:

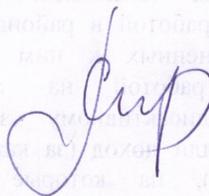
- ✓ анкетные и биографические данные;
- ✓ фотография;
- ✓ образование;
- ✓ сведения о трудовом и общем стаже;
- ✓ сведения о составе семьи;
- ✓ паспортные данные;
- ✓ сведения о воинском учете;
- ✓ сведения о заработной плате сотрудника;
- ✓ сведения о социальных льготах;
- ✓ специальность,
- ✓ занимаемая должность;
- ✓ наличие судимостей;
- ✓ адрес места жительства;
- ✓ домашний телефон;
- ✓ место работы или учебы членов семьи и родственников;
- ✓ содержание трудового договора;
- ✓ состав декларируемых сведений о наличии материальных ценностей;
- ✓ содержание декларации, подаваемой в налоговую инспекцию;
- ✓ подлинники и копии приказов по личному составу;
- ✓ личные дела и трудовые книжки сотрудников;
- ✓ основания к приказам по личному составу;

- ✓ дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- ✓ сведения о состоянии здоровья и иные медицинские сведения;
- ✓ иные необходимые данные:

№ п/п	Содержание сведений	Основание для включения в Перечень
1	Сведения о частной жизни, переписке, телефонных переговорах, почтовых, телеграфных, электронных и иных сообщениях личной и семейной тайне	Ст.23, 24 Конституции Российской Федерации
2	Информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (персональные данные)	Ст. 85 Трудового кодекса Российской Федерации
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	Ст.12 Федерального закона «Об актах гражданского состояния»
4	Сведения о доходах, об имуществе и обязательствах имущественного характера	Ст. 15 Федерального закона «О муниципальной службе в Российской Федерации»
5	Сведения о населении, содержащиеся в переписных листах	Ст. 8 Федерального закона «О Всероссийской переписи населения»
6	Сведения, содержащиеся в индивидуальных лицевых счетах застрахованных лиц: страховой номер; фамилия, имя и отчество; 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; гражданство; номер телефона; периоды трудовой и иной общественно полезной деятельности, включаемые в общий стаж для назначения государственной 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 стажа), на которые начислены страховые взносы в Пенсионный фонд Российской Федерации в соответствии с законодательством Российской Федерации; сумма заработка (за каждый месяц страхового стажа), который учитывается при назначении трудовой пенсии; сумма заработка (за каждый месяц страхового стажа), который учитывается при назначении трудовой пенсии; сумма начисленных	Ст.17 Федерального закона «Об индивидуальном персонифицированном учете в системе государственного пенсионного страхования»

	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 начислении пенсии пенсионного страхования	
7	Сведения, содержащиеся в регистрах бухгалтерского учета, внутренней бухгалтерской отчетности организаций	Ст.10 Федерального закона «О бухгалтерском учете»
8	Информация, полученная в ходе проверки финансово-хозяйственной деятельности лиц, осуществляющих внешнеэкономические операции с товарами, информацией, работами, услугами, результатами интеллектуальной деятельности	Ст.15,17 Федерального закона «Об экспортном контроле»
9	Сведения о налогоплательщике с момента постановки на учет, если иное не предусмотрено Налоговым кодексом	Ст.121 Налогового кодекса Российской Федерации, часть 110.
10	Содержание данных налогового учета в том числе данных первичных документов) является налоговой тайной)	Ст. 313 Налогового кодекса Российской Федерации, часть 2 11. 1.
11	1.Операторами и третьими лицами, получившими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением и случаев, предусмотренных частью 2 настоящей статьи. 2. Обеспечения конфиденциальности персональных данных не требуется: 1) в случае обезличивания персональных данных; 2) в отношении общедоступных персональных данных.	Ст.7 Федерального закона «О персональных данных»
12	Сведения о специальных средствах, технических приемах, тактике осуществления мероприятий по борьбе с терроризмом, а также о составе их участников	Ст. 2 Федерального закона «О противодействии терроризму»

Директор
МБОУ ДО «ЦРО»



Дожидаева Т.Г.

2. Приложение №1

к Положению о конфиденциальной информации

МБОУ ДО «ЦРО»

ОБЯЗАТЕЛЬСТВО о неразглашении конфиденциальной информации, не содержащей сведений, составляющих государственную тайну

Я, _____
(Ф.И.О. работника)

исполняющий(ая) должностные обязанности по замещаемой должности _____
(должность, наименование организации)

назначенный(ая) приказом _____
(кем назначен, наименование организации)

№ _____ от « _____ » _____ 20__ года, предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностной инструкцией (должностным регламентом) мне будет предоставлен допуск к конфиденциальной информации, не содержащей сведений, составляющих государственную тайну<1> (далее – конфиденциальные сведения), персональным данным отдельных категорий граждан<2>.

Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать<3>, не передавать и не раскрывать третьим лицам<4> конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей, за исключением случаев привлечения последних к деятельности, требующей раскрытия такой информации и только в объеме, необходимом для реализации целей и задач МБОУ ДО «ЦРО» ПМО далее – Учреждение), с письменного разрешения _____

(руководитель, наименование организации)

2. Выполнять, относящиеся ко мне требования внутренних организационно-распорядительных актов Учреждения в части оборота, неразглашения, нераспространения и защиты конфиденциальной информации.

3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному начальнику, а также лицу, ответственному за организацию защиты информации в Учреждении.

4. Не производить преднамеренных действий, нарушающих достоверность, целостность конфиденциальной информации Учреждения.

5. Не использовать ставшие мне известными или разработанные мною конфиденциальные сведения иначе, как в интересах Учреждения и не использовать их с целью получения выгоды.

6. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений, а также соблюдать правила и меры по защите конфиденциальной информации, указанные в Порядке обращения с

конфиденциальной информацией и средствами криптографической защиты информации в Учреждении и в других организационно-распорядительных правовых актах Учреждения.

7. В случае прекращения работы в Учреждении, сразу же возвратить Учреждению все документы и другие материалы, содержание которых отнесено к конфиденциальной информации, полученные мною в ходе выполнения своих служебных обязанностей.

8. После прекращения права на допуск к конфиденциальным сведениям, ставшие мне известные персональные данные не подлежат разглашению и передаче третьим лицам в течение неограниченного срока.

Я подтверждаю, что ознакомлен(а) с правилами и мерами по защите конфиденциальной информации, действующими в Учреждении и до моего сведения доведены с разъяснениями соответствующие требования Положения о конфиденциальной информации Учреждения.

Я подтверждаю, что не имею перед кем-либо никаких обязательств, которые входят в противоречие с настоящим обязательством или ограничивают мою деятельность в Учреждении.

Я предупрежден(а), что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной, административной или уголовной ответственности в соответствии с действующим законодательством.

(Ф.И.О.)

(подпись)

« ____ » _____ 20 ____ г.

<1> государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации (абзац 2 статьи 2 Федерального закона «О государственной тайне»).

<2> Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация (пункт 1 статьи 3 Федерального закона «О персональных данных»).

<3> Под разглашением понимается умышленное или неумышленное (неосторожное) действие лица, приведшие к ознакомлению (оглашению) с конфиденциальными сведениями лиц, не имеющих в установленном порядке допуска к конфиденциальным сведениям.

<4> Третьи лица - лица, не имеющие в установленном порядке допуска к конфиденциальным сведениям.

Правила об использовании электронной почты МБОУ ДО «ЦРО»

1. Общие положения

1. Настоящие правила регулируют порядок пользования работниками электронными адресами, зарегистрированными в домене @mail.ru и yandex.ru как корпоративные адреса электронной почты.

2. В рамках корпоративной почты используются следующие электронные адреса (далее адреса):

Официальные адреса структурных подразделений:

- cropmr@mail.ru – директор;
- do_cropit@mail.ru – отдел по предоставлению услуг дополнительного образования (ответственная за ведение эл.почты – заместитель директора Луковская Г.И.);
- pmssegorova@yandex.ru – отдел психолого-педагогических услуг (ответственная за ведение эл.почты - социальный педагог Ильина М.В.);
- zavxoz_cro@mail.ru – хозяйственный отдел (ответственная за ведение эл.почты - заведующий хозяйством Бузыкаева Е.В.);
- cro_spec1@mail.ru и metotdel.spec@mail.ru – отдел по работе с образовательными учреждениями (ответственная за ведение эл.почты - ведущий специалист Бушковская Г.М.).

Правила пользования корпоративными адресами и электронной почтой работниками МБОУ ДО «ЦРО»

1. Работник МБОУ ДО «ЦРО» имеет право пользоваться корпоративными адресами при осуществлении своих трудовых обязанностей, в том числе отправлять и получать электронные письма (далее – письма) внутренним и внешним корреспондентам с использованием адреса.

2. Работник МБОУ ДО «ЦРО» при подготовке электронного письма должен:

- 1) указывать тему письма, соответствующую его содержанию;
- 2) в случае, если к письму прилагаются файлы-вложения, указать на данное обстоятельство в основном тексте письма;
- 3) в конце письма разместить свою подпись (фамилию, имя, отчество), указание на свою должность, место работы, рабочий телефон, включая междугородный код города Питкяранта, корпоративный адрес.

Образец оформления электронного письма размещен в Приложении №1 к настоящим Правилам.

3. Работнику МБОУ ДО «ЦРО» запрещается:

- 1) использовать корпоративные адреса для целей, не связанных с исполнением трудовых обязанностей в МБОУ ДО «ЦРО»;
- 2) использовать для официальной и деловой переписки адреса электронной почты, не относящиеся к корпоративной почте;
- 3) осуществлять массовую рассылку писем внешним адресатам, в том числе писем рекламного характера;
- 4) рассылать письма, содержащие:
конфиденциальную информацию, доступ к которой ограничен законодательством, Положением о конфиденциальной информации МБОУ ДО «ЦРО», в том числе содержащую государственную тайну, коммерческую тайну, персональные

данные граждан в открытом виде (при отсутствии согласия последних), материалы, использование которых нарушает права на результаты интеллектуальной деятельности;

- недостоверную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, порочащую деловую репутацию, способствующую разжиганию национальной розни, призывающую к совершению противоправной деятельности и т.п.;

- файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования;

- программы для осуществления несанкционированного доступа;
- серийные номера к программным продуктам и программы для их генерации;
- логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете;

- ссылки на вышеуказанную информацию.

5) без разрешения директора МБОУ ДО «ЦРО»:

- использовать адрес корпоративной почты для оформления подписок на почтовые рассылки;

- публиковать любые адреса, используемые в рамках корпоративной почты, на общедоступных Интернет-ресурсах;

- сообщать пароль доступа к своему почтовому ящику любым другим лицам.

- удалять (исправлять) любую входящую (исходящую) корреспонденцию и сообщения.

4. При систематическом (два и более раза) нарушении запретов, указанных в пунктах 3 и 6 настоящих Правил, работник МБОУ ДО «ЦРО» может быть привлечен к дисциплинарной ответственности.

5. Работнику МБОУ ДО «ЦРО» рекомендуется регулярно (не реже одного раза каждые 3 часа в течение рабочего времени) проверять поступление почты на свой индивидуальный адрес.

6. Работник обязан обо всех внештатных ситуациях, несанкционированных перемещения (удалениях) писем, сообщений, взломе п\я и т.д. немедленно уведомлять директора МБОУ ДО «ЦРО».

III. Правила организации деятельности электронной почты

1. Функционирование корпоративной почты обеспечивают ответственные сотрудники отделов.

2. Директор (или иное уполномоченное лицо):

- ведет учет адресов, мониторинг пользования корпоративных адресов;
- обеспечивает создание, блокирование и ликвидацию адресов;

- осуществляет сбор и хранение всех паролей от официальных почтовых ящиков сотрудников МБОУ ДО «ЦРО» и номера телефонов «привязанных» к этим почтовым ящикам (далее п\я), для их восстановления.

- в случае увольнения сотрудника, в день его увольнения, в присутствии самого работника, удаляет телефон увольняющегося сотрудника из списка «привязанных» к п\я, проверяет почтовый ящик, «привязывает» свой номер телефона, как дополнительный для восстановления пароля и производит смену пароля;

- при служебной необходимости принимает решение о создании индивидуального п\я работника в МБОУ ДО «ЦРО». Ликвидация индивидуального адреса работника МБОУ ДО «ЦРО» осуществляется при его увольнении, смене им фамилии, а также при систематическом нарушении работником настоящих Правил;

- может разрешить работнику, в исключительных случаях, работать с личного почтового ящика. В этом случае работник должен создать отдельную папку в своем п\я, куда переносить всю служебную корреспонденцию. Для папки рекомендуется установить пароль. Работник обязан сообщать обо всей служебной корреспонденции исходящей и

входящей, отправленной (принятой) в его личный п/я. Вся исходящую служебную корреспонденцию из личного п/я работник обязан направлять адресату с копией на п/я директора cropmr@mail.ru. По запросу директора работник должен разрешить проверку служебной папки своего п/я.

3. В целях контроля настоящих Правил, содержимое почтового ящика работника МБОУ ДО «ЦРО» может быть проверено директором или иным уполномоченным лицом без предварительного уведомления работника.

4. Индивидуальные адреса работников блокируются в случаях:

- осуществления рассылки писем, содержащих вредоносные программы, спам, информацию, распространение которой запрещено нормативными правовыми актами;
- возможности доступа к соответствующим почтовым ящикам третьих лиц;
- использования работником корпоративной почты не по назначению;
- в иных случаях нарушения настоящих Правил, по решению директора

МБОУ ДО «ЦРО» ПМО

Директор
МБОУ ДО «ЦРО»

Дожидаева Т.Г.

1. Приложение №1
к Правилам пользования
электронной почтой
в МБОУ ДО «ЦРО»

ОБРАЗЕЦ
оформления электронного письма

Адресат: cro_spec1@mail.ru, pmssegorova@yandex.ru

Тема: [Правила пользования корпоративной электронной почтой]

Тело письма:

[Добрый день, уважаемые коллеги!

Предлагаю вашему вниманию Правила пользования корпоративной электронной почтой.

Необходимость в правилах стала очевидной в связи с несанкционированным удалением из почты сообщений.

Правила пользования корпоративной электронной почтой в прилагаемом файле – «Правила пользования корпоративной электронной почтой.docx».]

Подпись:

[С уважением,

Директор

МБОУ ДО «ЦРО» Дожидаева Т.Г.

(8814-33) 4-21-14,

e-mail: croprn@mail.ru

4. Приложение №4
к Положению о конфиденциальной информации
Директору МБОУ ДО «ЦРО»
Дожидаевой Т.Г.

От _____
ФИО

СОГЛАСИЕ
на обработку персональных данных

Я, _____,
(фамилия, имя, отчество субъекта персональных данных)

, зарегистрирован по адресу: _____,

документ, удостоверяющий личность: _____,

(наименование документа, №, сведения о дате выдачи документа и выдавшем его органе)

в целях _____,

(указать цель обработки данных)

в соответствии с п. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", выражаю согласие МБОУ ДО «ЦРО» ПМО расположенному по адресу: 186810, Республика Карелия, г.Питкяранта, ул.Ленина, дом 38А, на обработку (сбор, накопление, систематизацию, хранение, уточнение (обновление, изменение), использование, распространение (передачу третьим лицам), обезличивание, блокировку и уничтожение) моих персональных данных, то есть на совершение действий, предусмотренных п.3, ст.3 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных".

Перечень моих персональных данных, на обработку которых я даю согласие:

- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения;
- паспортные данные;
- адрес регистрации по месту жительства и адрес фактического проживания;
- номер телефона (домашний, мобильный);
- данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;
- семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым и налоговым законодательством;
- отношение к воинской обязанности;
- сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;
- СНИЛС;
- ИНН;
- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в ООО МБОУ ДО «ЦРО» ,
- сведения о доходах в МБОУ ДО «ЦРО»
- сведения о деловых и иных личных качествах, носящих оценочный характер.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

" ____ " _____ Г.

ФИО Субъекта персональных данных:

_____ / _____

Приложение №5
к Положению о конфиденциальной информации
Директору МБОУ ДО «ЦРО»
Дожидаевой Т.Г.
От _____
(ФИО родителя (законного представителя)
обучающегося)

**ЗАЯВЛЕНИЕ-СОГЛАСИЕ
на обработку персональных данных**

Я, _____,
(фамилия, имя, отчество субъекта персональных данных)
зарегистрирован _____ по адресу: _____

документ, удостоверяющий личность: _____

(наименование документа, №, сведения о дате выдачи документа и выдавшем его органе)

в соответствии с п. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", выражаю согласие МБОУ ДО «ЦРО» ПМО расположенному по адресу: 186810, Республика Карелия, г.Питкяранта, ул.Ленина, дом 38А, на обработку (сбор, накопление, систематизацию, хранение, уточнение (обновление, изменение), использование, распространение (передачу третьим лицам), обезличивание, блокировку и уничтожение) моих персональных данных, персональных данных моего ребенка (воспитанника)

ФИО,

дата рождения, № свидетельства о рождении, СНИЛС, ИНН,

то есть на совершение действий, предусмотренных п.3, ст.3 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", для обработки в целях:
заключения договора на оказание образовательных услуг моему ребенку; получения образовательных услуг моим ребенком; проведения тренинга и тестирования (в том числе психологического); получение медицинских услуг моим ребенком; получение услуги ПМПК; проведение фото-видеосъемки с участием моего ребенка.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

" ____ " _____ г.

ФИО родителя (законного представителя) обучающегося:

/ _____