****

**Муниципальное дошкольное образовательное учреждение № 30 «Буратино»**

**поселка Чульман Нерюнгринского района**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

678981, Республика Саха (Якутия), Нерюнгринский район, поселок Чульман, ул. Гагарина 27а,

тел: (8-41147) 7-61-20 buratino@nerungri.edu.ru

**Приказ**

от22октября2019г. № 61

**«Обответственномлицезаинформационнуюбезопасностьдошкольногообразовательногоучреждения»**

РуководствуясьтребованиямиФедеральногозаконаот 29.12.2010№436—ФЗ

«О защите детей от информации, причиняющей вред их здоровью и развитию»(сизменениямиот2012г),Федеральногозаконаот27.07.2006№152«Оперсональных данных» с целью обеспечения режима конфиденциальности, вцелях осуществления ограничения доступа работников детского учреждения кресурсамиматериаламсетиИнтернет,неимеющихотношениякобразовательномупроцессу,вцеляхобеспеченияинформационнойбезопасностив ДОУ

Приказываю:

1. Назначить ответственногозаинформационнуюбезопасность вДОУ

учителя-логопеда Кривоногову И.Ю.

1. Утвердитьиввестивдействие

Положение об информационной безопасности

Положение об ответственном лице за информационную

безопасность (Приложение 1)

Инструкцию для сотрудников МДОУ о порядке действий при осуществлении контроля

за использованием работниками учреждения сети Интернет (Приложение 2)

1. Ознакомитьсприказомвсехработников МДОУ
2. Разместить настоящий приказ наофициальном сайте учреждения втечении10рабочихднейсодняегоиздания
3. Контроль за исполнением оставляю за собой

Заведующая МДОУ № 30 «Буратино» А.В.Головченко

**Приложение№1**

**кприказу№61**

**от«22» октября2019г.**

**Положениеобответственномлицезаинформационнуюбезопасность**

**Муниципального дошкольного образовательного учреждения № 30 «Буратино»**

**поселка Чульман Нерюнгринского района**

1. ***Общиеположения***

Ответственноелицозаинформационнуюбезопасностьдошкольногообразовательногоучреждения(далееОператор)назначаетсявцеляхвыполнениятребованийдействующегозаконодательстваРоссийскойФедерации,иныхнормативно-правовыхактов,регламентирующихобеспечение защиты информации, в том числе обеспечение безопасности приобработке персональных данных, а также обеспечение защиты и безопасностиинформационныхтехнологийитехническихсредств,позволяющихосуществлятьобработкутакихперсональныхданных.

1. ***Структура***

Ответственное лицо за информационную безопасность дошкольногообразовательногоучрежденияназначаетсяприказомзаведующегоДОУ.

1. ***Задачи***

Основныезадачиответственноголицазаключаютсявследующем.

1. Разработкаиреализациякомплексаорганизационныхитехнических мер, направленных на выполнение установленных требований кобеспечению безопасности и защите информации, в том числе персональныхданных.
2. ОбеспечениепостоянногоконтролявподразделенияхОператораза выполнениемустановленныхтребованийк обеспечениюбезопасностиизащитеинформации,втомчислеперсональныхданных.
3. Разработкаивнесениепредложенийпосовершенствованиюиразвитиюкорпоративнойсистемыобеспечениябезопасностиизащитыинформации,втомчислеперсональныхданных.
4. ***Функции***

Длявыполненияпоставленных задачосуществляетследующиефункции.

1. Готовитипредставляетнарассмотрениеруководствупроектылокальныхнормативныхактовповопросамобеспечениязащитыинформации,в томчислеперсональныхданных.
2. Организуетипроводитвовзаимодействиисзаинтересованнымиподразделениями классификациюинформационных системна этапесозданияинформационных систем или в ходе их эксплуатации (для ранее введенных вэксплуатациюи(или)модернизируемых информационных систем)с цельюустановленияметодовиспособовзащитыинформации,необходимыхдляобеспечения безопасности персональных данных в соответствии сустановленными требованиями.
3. Разрабатываетиреализуеткомплексорганизационныхимерпообеспечениюзащитыинформацииот:

неправомерногодоступа;

уничтожения;

модифицирования;

блокирования;

копирования;

предоставления;

распространения;

а также от иных неправомерных действий в отношении такойинформации.

 4. Длязащитыинформации,в том числеперсональныхданныхотнеправомерногодоступаобеспечивает:

контрользастрогимсоблюдениемпринятогоПорядкадоступакконфиденциальной информации,в томчислек персональнымданным;предотвращениенесанкционированногодоступакинформациии(или)передачиеелицам,неимеющимправанадоступкинформации;своевременное обнаружение фактовнесанкционированногодоступа кинформации;

предупреждениевозможностинеблагоприятныхпоследствийнарушенияпорядкадоступакинформации;-возможностьнезамедлительноговосстановленияинформациимодифицированной или уничтоженнойвследствиенесанкционированногодоступакней.

1. Ответственноелицоприсозданиииэксплуатациикорпоративныхинформационныхсистем:

- самостоятельноразрабатываетивнедряетметодыиспособызащиты информации, соответствующие установленным требованиям; -согласовываетисполнителюпланируемыедля использованияв целяхзащиты информации методы и способы при условии их соответствияустановленнымтребованиям.

- разрабатываети реализует меры организационного и технического понедопущению воздействия на технические средства обработки информации, врезультатекоторогонарушаетсяихфункционирование;

- организуети(или)проводитэкспертизутехническихсредств,используемыхприобработкеинформациинапредметсоответствия

возможностейзащитыинформацииуказанныхсредствустановленнымтребованиям.

1. Разрабатывает и реализует меры по информированию и обучениюперсонала Оператора, в том числе вновь принимаемых на работу лиц, повопросамзащитыинформациии персональныхданных.
2. Контролируетвыполнениеустановленныхтребованийпо:

- осуществлению обмена персональными данными при их обработке винформационныхсистемахпоканаламсвязи,защитакоторыхобеспечиваетсяпутем реализации соответствующих организационных мер и(или) путемприменениятехнических средств;

- размещению информационных систем, специального оборудования иохране помещений, в которых ведется работа с персональными данными,организации режима обеспечения безопасности в этих помещениях в частиобеспечениясохранностиносителейперсональныхданныхисредствзащитыинформации, а также исключения возможности неконтролируемогопроникновенияилипребываниявэтихпомещенияхпостороннихлиц;

- соблюдениюпарольнойзащиты;

- соблюдениюустановленногорегламентаработысэлектроннойпочтой;

- соблюдениютребованийкпрограммномуобеспечениюиегоиспользованию.

 8. Всоответствиисустановленныминормативно-правовымиактамитребованиямиобеспечивает:

- определениеугрозбезопасностиперсональныхданныхприихобработке,формированиена ихосновемоделиугроз;

- разработку на основе модели угроз системы защиты персональныхданных, обеспечивающей нейтрализацию предполагаемых угроз сиспользованием методов и способов защиты персональных данных,предусмотренныхдлясоответствующегоклассаинформационныхсистем;

- проверку готовности средств защиты информации к использованию ссоставлениемзаключенийовозможностиихэксплуатации;

- установку и ввод в эксплуатацию средств защиты информации всоответствиисэксплуатационнойитехническойдокументацией;

- обучение лиц, использующих средства защиты информации,применяемыевинформационныхсистемах,правиламработысними;

- учетприменяемыхсредствзащитыинформации,эксплуатационнойитехническойдокументациикним,носителейперсональныхданных;

- учетлиц,допущенныхкработесперсональнымиданнымивинформационнойсистеме;

- контрользасоблюдениемусловийиспользованиясредствзащитыинформации, - предусмотренных эксплуатационной и техническойдокументацией;

- разбор и составление заключений по фактам несоблюдения условийхраненияносителейперсональныхданных,использованиясредствзащитыинформации,которыемогутпривестикнарушениюконфиденциальностиперсональныхданныхилидругимнарушениям,приводящимкснижениюуровня защищенностиперсональныхданных, разработку и принятие мер попредотвращениювозможныхопасныхпоследствийподобныхнарушений;

- описание системы защиты информации, втом числе персональныхданных;

ежегодное планирование работы по совершенствованию системызащитыинформации,втомчислеперсональныхданных;

- подготовкуипредоставлениеотчетовзаведующему,атакжепотребованиюнадзорныхи иных уполномоченных органов об организационныхитехническихмероприятияхпозащитеинформации,втомчислеперсональныхданных;

- постоянныйконтрользаобеспечениемуровнязащищенностиинформации.

***5. Взаимодействие***

ДлярешенияпоставленныхзадачиосуществленияпредусмотренныхнастоящимПоложениемфункцийОтветственноелицовзаимодействует:

- сруководителемДОУ иегозаместителями;

- слюбымииными подразделениями;

- сгосударственными,муниципальнымиорганами,учреждениямииорганизациями,снадзорнымиорганами,атакжесинымиорганами,предприятиямииорганизациями.

1. ***Ответственность***

ОтветственноелицозаинформационнуюбезопасностьнесетответственностьпередруководствомДОУсогласнодействующемузаконодательству, нормативно-правовым и локальным нормативным правовымактамзаобеспечение:

- выполненияпоставленныхпередподразделениемзадачифункций,

работысдокументамииихсохранности,своевременногоикачественногоисполненияпорученийи обращений,

- выполнениятребованийправилвнутреннеготрудовогораспорядка,

- соблюдениявподразделенииправилпротивопожарнойбезопасности.

требованийвыполнениядействующегозаконодательстваРоссийскойФедерации,иныхнормативно-правовыхдокументов,регламентирующихобеспечение защиты информации, в том числе обеспечение безопасности приобработкеперсональныхданных;

- обязанностей,предусмотренныхТрудовымкодексомРФ,правиламивнутреннеготрудовогораспорядка,коллективнымдоговором,настоящимПоложением,трудовымидоговорамиидолжностнымиинструкциями.

**Приложение№2**

**кприказу№61**

**от«22» октября2019г.**

# ИНСТРУКЦИЯ

**для сотрудников образовательного учреждения о порядке действий приосуществленииконтролязаиспользованиемработникамиучреждениясетиИнтернет**

1. НастоящаяИнструкцияустанавливаетпорядокдействийприобнаружениисотрудникамиобразовательногоучреждения:

- возможности доступа работников учреждения к потенциально опасномуконтенту;

- вызванного техническими причинами отказа доступа к контенту, непредставляющему опасности работников учреждения, доступ к которому непротиворечитпринятымнормативнымактамнафедеральномуровне,атакженауровне образовательногоучреждения.

 2. Контроль за использованием работниками учреждения сети Интернетосуществляют ответственные лица во время использования сети Интернет длясвободной работы работников учреждения– администратор точки доступа ксетиИнтернет вобразовательномучреждении.

 3. Ответственное лицо, осуществляющее контроль за использованиемработникамиучреждения сетиИнтернет:

- определяетвремяиместоработыработниковучреждениявсетиИнтернетсучетомиспользованиясоответствующихтехническихвозможностейв образовательном процессе, а также длительность сеанса работы одногоработникаучреждения;

- способствуетосуществлениюконтролязаобъемомтрафикаобразовательногоучреждениявсетиИнтернет;

- наблюдаетзаиспользованиемкомпьютеровисетиИнтернетработникамиучреждения;

- запрещает дальнейшую работу работника учреждения в сети Интернет вслучае нарушения работником учреждения порядка использования сетиИнтернет и предъявляемых работникам учреждения требований при работе всетиИнтернет;

- недопускаетработникаучреждениякработевсетиИнтернетвпредусмотренныхПравиламииспользованиясетиИнтернетслучаях;

- принимает необходимые меры для пресечения дальнейших попытокдоступакресурсу/группересурсов,несовместимыхсзадачамиобразования.

 4. При обнаружении информации, в отношении которой у лица,осуществляющего контроль за использованием работниками учреждения сетиИнтернет,возникаютоснованияпредполагать,чтотакаяинформацияотноситсяк числу запрещенной для распространения в соответствии с законодательствомРоссийской Федерации или иному потенциально опасному для работниковучрежденияконтенту,ответственноелицоинформируетадминистратораточки

доступаксетиИнтернетилируководителяобразовательногоучреждения,которыепринимают необходимыерешения.

5.При обнаружении вызванного техническими причинами отказадоступакконтенту,доступ

ккоторомунепротиворечит принятымнормативным актам на федеральном уровне, уровне субъекта РоссийскойФедерации, муниципальном уровне, а также на уровне образовательногоучреждения,ответственноелицоинформируетсоответствующиетехническиеслужбы,осуществляющиеконтентнуюфильтрацию.