Муниципальное образовательное учреждение дополнительного образования
«Центр дополнительного образования детей»
152613, Ярославская область, г. Углич, ул. З.Золотовой, д. 42

Утверждаю
Директор МОУ ДО «Центр
дополнительного образования детей»
_____М.Л.Буцких
«__» _____20__г.

Политика информационной безопасности муниципального образовательного учреждения дополнительного образования «Центр дополнительного образования детей»

1. Общие положения

1.1. Политика информационной безопасности муниципального образовательного учреждения дополнительного образования «Центр дополнительного образования детей» (далее соответственно – Политика, Учреждение), разработана в соответствии с требованиями действующего законодательства и нормативных актов Российской Федерации:

– Федерального закона от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите и информации»,
– Федерального закона от 27 июля 2006 № 152-ФЗ «О персональных данных»,
– Федерального закона от 06 апреля 2011 № 63-ФЗ «Об электронной подписи»,
– Указа Президента Российской Федерации от 06 марта 1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»,
– Постановления Правительства РФ №1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
– Постановления Правительства РФ № 687 от 15.09.2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,
– приказа Минкомсвязи России от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию»,
– а также ряда иных нормативных правовых актов в сфере защиты информации.

1.2. Политика определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности, которыми руководствуются работники Учреждения при осуществлении своей деятельности.

1.3. Выполнение требований Политики является обязательным для всех работников Учреждения.

1.4. Ответственность за соблюдение информационной безопасности несет каждый работник Учреждения.

2. Цели и задачи Политики информационной безопасности

2.1. Основными целями Политики являются:

– сохранение конфиденциальности критичных информационных ресурсов;
– обеспечение непрерывности доступа к информационным ресурсам Учреждения;
– защита целостности информации с целью поддержания возможности Учреждения по оказанию услуг высокого качества и принятию эффективных

управленческих решений;

– повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Учреждения;

– определение степени ответственности и обязанностей работников по обеспечению информационной безопасности в Учреждении;

– повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз информационной безопасности;

– предотвращение и/или снижение ущерба от инцидентов информационной безопасности.

2.2. Основными задачами Политики являются:

– разработка требований по обеспечению информационной безопасности;

– контроль выполнения установленных требований по обеспечению информационной безопасности;

– повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию информационной безопасности;

– разработка нормативных документов для обеспечения информационной безопасности Учреждения;

– выявление, оценка, прогнозирование и предотвращение реализации угроз информационной безопасности Учреждения;

– организация антивирусной защиты информационных ресурсов Учреждения;

– защита информации Учреждения от несанкционированного доступа и утечки по техническим каналам связи;

– организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору Учреждения.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика Учреждения направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий работников Учреждения, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

3.2. Наибольшими возможностями для нанесения ущерба обладает собственный персонал Учреждения. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией работников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

3.3. Стратегия обеспечения информационной безопасности Учреждения заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий работников Учреждения.

4. Основные принципы обеспечения информационной безопасности

4.1. Основными принципами обеспечения информационной безопасности являются:

– постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов Учреждения;

– своевременное обнаружение проблем, потенциально способных повлиять на информационную безопасность Учреждения, корректировка моделей угроз и нарушителя;

– разработка и внедрение защитных мер;

– контроль эффективности принимаемых защитных мер;

– персонификация и разделение ролей и ответственности между работниками Учреждения за обеспечение информационной безопасности Учреждения исходит из

принципа персональной и единоличной ответственности за совершаемые операции.

5. Объекты защиты

5.1. Объектами защиты с точки зрения информационной безопасности в Учреждении являются:

– информационный процесс профессиональной деятельности;

– информационные активы Учреждения.

5.2. Защищаемая информация делится на следующие виды:

– информация по финансово-экономической деятельности Учреждения;

– 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;

– другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

6. Требования по информационной безопасности

6.1. В отношении всех собственных информационных активов Учреждения, активов, находящихся под контролем Учреждения, а также активов, используемых для получения доступа к инфраструктуре Учреждения, должна быть определена ответственность соответствующего работника Учреждения.

6.2. Все работы в пределах Учреждения должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в Учреждении.

6.3. Внос в здание и помещения Учреждения личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы Учреждения производится только при согласовании с директором Учреждения.

6.4. Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну Учреждения и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

6.5. В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля. Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким.

6.6. Каждый работник обязан немедленно уведомить директора Учреждения обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети. Доступ третьих лиц к информационным системам Учреждения должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам Учреждения должен быть четко определен, контролируем и защищен.

6.7. Работникам, использующим в работе портативные компьютеры Учреждения, может быть предоставлен удаленный доступ к сетевым ресурсам Учреждения в соответствии с правами в корпоративной информационной системе.

6.8. Работникам, работающим за пределами Учреждения с использованием компьютера, не принадлежащего Учреждению, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

6.9. Работники, имеющие право удаленного доступа к информационным ресурсам Учреждения, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети Учреждения и к каким-либо другим сетям, не принадлежащим Учреждению.

6.10. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Учреждения, должны иметь программное обеспечение

антивирусной защиты, имеющее последние обновления.

6.11. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

6.12. Рекомендованные правила:

– работникам Учреждения разрешается использовать сеть Интернет только в служебных целях;

– запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

– работники Учреждения не должны использовать сеть Интернет для хранения корпоративных данных;

– работа с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Учреждения в сеть Интернет;

– работникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Учреждению;

– работники Учреждения перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

– запрещен доступ в Интернет через сеть Учреждения для всех лиц, не являющихся работниками Учреждения, включая членов семьи работников Учреждения.

6.13. Директор Учреждения имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

6.14. Работники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация Учреждения.

6.15. Работникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит системный администратор Учреждения.

6.16. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа "мышь", шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей Политики вместе именуются "компьютерное оборудование". Компьютерное оборудование является собственностью Учреждения и предназначено для использования исключительно в производственных целях.

6.17. Каждый работник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

6.18. Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима "Экранной заставки". Для установки режимов защиты пользователь должен обратиться к инженеру-программисту Учреждения. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

6.19. Все программное обеспечение, установленное на компьютерном оборудовании Учреждения, является собственностью Учреждения и должно использоваться исключительно в рабочих целях.

6.20. Работникам Учреждения запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное

обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности.

6.21. На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

- персональный межсетевой экран;
- антивирусное программное обеспечение;
- программное обеспечение шифрования жестких дисков.

6.22. Работники Учреждения не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

6.23. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Работникам запрещается направлять конфиденциальную информацию Учреждения по электронной почте без использования систем шифрования. Строго конфиденциальная информация Учреждения, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

6.28. Использование работниками Учреждения публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации локальной вычислительной сети при условии применения механизмов шифрования.

6.29. Работники Учреждения для обмена документами должны использовать только свой официальный адрес электронной почты.

6.30. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций. В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать директора Учреждения. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

6.31. Не допускается при использования электронной почты:

– рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;

– рассылка рекламных материалов;

– подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;

– поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);

– пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам в области этики.

6.32. Объем пересылаемого сообщения по электронной почте не должен превышать 2 Мбайт.

6.33. Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

6.34. В случае кражи переносного компьютера следует незамедлительно сообщить директору Учреждения.

6.35. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения работник обязан:

– проинформировать директора и системного администратора Учреждения;

– не пользоваться и не выключать зараженный компьютер;

– не подсоединять этот компьютер к компьютерной сети Учреждения до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование системным администратором.

6.36. Работникам Учреждения запрещается:

– нарушать информационную безопасность и работу сети Учреждения;

– сканировать порты или систему безопасности;

– контролировать работу сети с перехватом данных;

– получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;

– использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;

– передавать информацию о работниках или списки работников Учреждения посторонним лицам;

– создавать, обновлять или распространять компьютерные вирусы и прочее разрушительное программное обеспечение.

6.41. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

6.42. Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

6.43. Только системный администратор Учреждения может создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним по согласованию с директором Учреждения.

6.44. Работники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

6.45. Все заявки на проведение технического обслуживания компьютеров должны направляться системному администратору Учреждения.

6.46. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, и согласованны с системным администратором Учреждения.

7. Управление информационной безопасностью

7.1. Управление информационной безопасностью Учреждения включает в себя:

– разработку и поддержание в актуальном состоянии Политики информационной безопасности;

– разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению информационной безопасности;

- обеспечение бесперебойного функционирования комплекса средств информационной безопасности;
- осуществление контроля (мониторинга) функционирования системы информационной безопасности;
- оценку рисков, связанных с нарушениями информационной безопасности.

8. Реализация Политики информационной безопасности

8.1. Реализация Политики Учреждения осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности.

9. Порядок внесения изменений и дополнений в Политику информационной безопасности

9.1. Внесение изменений и дополнений в Политику производится не реже одного раза в три года с целью приведения в соответствие определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

10. Контроль за соблюдением Политики информационной безопасности

10.1. Текущий контроль за соблюдением выполнения требований Политики Учреждения возлагается на работника, назначенного приказом директора Учреждения.

10.2. Директор Учреждения на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики, а также осуществляет последующий контроль за соблюдением ее требований.