СОГЛАСОВАНО:
Председатнель ПК
_____ Г.Ф.Антропьева

УТВЕРЖДАЮ:
Заведующий БДОУ
_____ С.В.Силинская
«28» 09 2020 г

ПРИНЯТО: Общим собранием трудового коллектива 29.09.2020г

ПОЛОЖЕНИЕ
об информационной безопасности БДОУ «Тарногский детский сад комбинированного вида №2 «Солнышко»

2020г

Основные понятия:
Сеть Интернет представляет собой глобальное объединение компьютерных сетей и информационных ресурсов, принадлежащих множеству различных людей и организаций. Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности.
Пользователь сети Интернет – лицо, использующее ресурсы всемирной компьютерной сети.

1.Общие положения.

1.1. Настоящее Положение об информационной безопасности (далее — Положение) Бюджетного дошкольного образовательного учреждения Тарногского муниципального района Вологодской области «Тарногский детский сад комбинированного вида №2 «Солнышко» (далее- ДОУ) разработано в соответствии с Федеральный закон от 29 декабря 2012 г N 273 ФЗ Об образовании в РФ», 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» (в редакции от 28.06.2010 г.), Федеральным законом РФ от 29 декабря 2010 г № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Распоряжением Правительства РФ от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей», Приказом Минкомсвязи России от 27.02.2018 N 88 «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018 - 2020 годы», Письмом Минобрнауки России от 14.05.2018 N 08-1184 «О направлении информации» (вместе с «Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети «Интернет»)

1.2. Использование сети Интернет в образовательном учреждении направлено на решение задач учебно-воспитательного процесса.
Доступ к сети Интернет должен осуществляться только с использованием лицензионного программного обеспечения или программного обеспечения, разрешенного для свободного использования.
Настоящее Положение регулирует условия и порядок использования сети Интернет в дошкольном образовательном учреждении (ДОУ).
Настоящее Положение имеет статус локального нормативного акта дошкольного образовательного учреждения.

1.3. Вопросы использования возможностей сети Интернет в учебно-воспитательном процессе рассматриваются на педагогическом совете. Педагогический совет утверждает Регламент использования сети Интернет.

1.4. Руководитель образовательного учреждения отвечает за обеспечение пользователям (сотрудникам и обучающимся) эффективного и безопасного доступа к сети Интернет. Для обеспечения доступа к Сети участникам образовательного процесса руководитель ДОУ назначает своим приказом ответственных лиц из числа сотрудников образовательного учреждения за организацию работы с Интернетом и ограничение доступа.

1.5. Во время НОД и других видов детской деятельности контроль использования обучающимися сети Интернет осуществляет воспитатель, ведущий занятие.

1.6. При использовании сети Интернет в ДОУ учащимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации, и которые имеют прямое отношение к образовательному процессу. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в ДОУ или предоставленного оператором услуг связи.

1.7. Пользователи сети Интернет в ДОУ должны учитывать, что технические средства и программное обеспечение не могут обеспечить полную фильтрацию ресурсов сети

Интернет вследствие частого обновления ресурсов, поэтому ДОУ не несет ответственности за случайный доступ к подобной информации, размещенной не на Интернет-ресурсах ДОУ.
При обнаружении указанной информации пользователю необходимо сообщить об этом ответственному за использование сети Интернет в ДОУ, указав при этом адрес ресурса.
1.8. Принципы размещения информации на Интернет-ресурсах ДОУ призваны обеспечить:
- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защиту персональных данных участников образовательного процесса;
- достоверность и корректность информации.
1.9. Персональные данные обучающихся (включая фамилию и имя, группу/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр., иные сведения личного характера) могут размещаться на интернет-ресурсах только с письменного согласия родителя(законного представителя) обучающихся.
В информационных сообщениях о мероприятиях, размещенных на сайте ДОУ без уведомления и получения согласия упомянутых лиц или их законных представителей, могут быть указаны лишь фамилия и имя обучающегося, либо фамилия, имя и отчество сотрудника или родителя.
При получении согласия на размещение персональных данных, представитель ДОУ обязан разъяснить возможные риски и последствия их опубликования. ДОУ не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на опубликование персональных данных.

2. Права, обязанности и ответственность пользователей

Педагоги, сотрудники и обучающихся могут бесплатно пользоваться доступом к глобальным Интернет-ресурсам по разрешению лица, назначенного ответственным за организацию в ДОУ работы сети Интернет и ограничению доступа.
Пользователям запрещается:
1. Осуществлять действия, запрещенные законодательством РФ.
2. Посещать сайты, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (порнография, эротика, пропаганда насилия, терроризма, политического и религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности).
3. Загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.
4. Загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом.
5. Передавать информацию, представляющую коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство граждан.
6. Устанавливать на компьютерах дополнительное программное обеспечение, как полученное в Интернете, так и любое другое без специального разрешения.
7. Изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и всех программ, установленных на нем.
8. Осуществлять действия, направленные на "взлом" любых компьютеров,

находящихся как в «точке доступа к Интернету» ДОУ, так и за его пределами.
9. Использовать возможности «точки доступа к Интернету» ДОУ для пересылки и записи непристойной, клеветнической, оскорбительной, угрожающей и порнографической продукции, материалов и информации.
10. Осуществлять любые сделки через Интернет.
Пользователи несут ответственность:
1. За содержание передаваемой, принимаемой и печатаемой информации.
2. За нанесение любого ущерба оборудованию в «точке доступа к Интернету» (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.
3. При случайном обнаружении ресурса, содержание которого не имеет отношения к образовательному процессу, следует незамедлительно сообщить об этом преподавателю, проводящему занятие. Преподаватель обязан зафиксировать доменный адрес ресурса, время его обнаружения и сообщить об этом лицу, ответственному за работу сети и ограничение доступа к информационным ресурсам с тем, чтобы этот ресурс был занесен в общий список запрещенных ресурсов.
Пользователи имеют право:
1. Работать в сети Интернет в течение периода времени, определенного Правилами ДОУ.
2. Сохранять полученную информацию на съемном накопителе.
3. Размещать собственную информацию в сети Интернет на Интернет-ресурсах ДОУ.

3. Задачи, функции, обязанности, ответственность и права ответственных лиц за информационную безопасность ДОУ.

3.1. Ответственный за информационную безопасность подчиняются непосредственно заведующему ДОУ.
3.2. Ответственный за информационную безопасность в своей работе руководствуется настоящим Положением.
3.3. Ответственный за информационную безопасность в пределах своих функциональных обязанностей обеспечивает безопасность информации, обрабатываемой, передаваемой и хранимой при помощи информационных средств в ДОУ.
3.4. Основными задачами ответственного за информационную безопасность являются:
- Организация эксплуатации технических и программных средств защиты информации.
- Текущий контроль работы средств и систем защиты информации.
- Организация и контроль резервного копирования информации.
3.5. Ответственный за информационную безопасность выполняют следующие основные функции:
- Разработка инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете.
- Обучение персонала и пользователей персональным компьютером (далее – ПК) правилам безопасной обработки информации и правилам работы со средствами защиты информации.
- Организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в ДОУ.
- Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.
- Контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём.
- Контроль за санкционированным изменением программного обеспечения,

заменой и ремонтом ПК.
- Контроль пользования Интернетом.
3.6.Ответственный за информационную безопасность обязан обеспечить:
- функционирование и поддержание работоспособности средств и систем защиты информации в пределах возложенных на них обязанностей;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права пользователей на доступ к информации;
- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- адекватную оценку риска при использовании информационной системы организации, осведомленность об угрозах;
- знание внутренних процессов организации;
- установление целей и критериев безопасности информационной системы исходя из политики безопасности работодателя;
- анализ, аудит и мониторинг строгого соблюдения процедур безопасности информационной системы в организации;
- выработку и систематическое обновление локальных актов, их доведение до сотрудников организации;
- координацию расследования инцидентов;
- ежемесячный отчет о состоянии безопасности информационной системы ДОУ.
3.7.Совместно с организацией осуществляющей работы по техническому обслуживанию и поддержке сайта ДОУ обеспечить:
- защиту информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- незамедлительное восстановление информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- восстановление работоспособности средств и систем защиты информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- постоянный контроль за обеспечением уровня защищенности информации.
- Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку компьютеров на наличие вирусов.
- Сообщать незамедлительно заведующему ДОУ о выявлении случаев несанкционированного доступа в Интернет.
3.8 Права ответственного за информационную безопасность.
- Требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения.
- Готовить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов.
3.9.Ответственность лица, ответственного за информационную безопасность.
- На ответственного за информационную безопасность ДОУ возлагается персональная ответственность за качество проводимой им работы по обеспечению защиты информации в соответствии с функциональными обязанностями, определенными настоящим Положением.