Приложение 8

УТВЕРЖДАЮ
Директор МОБУ «Муринская СОШ № 6»
_____О.А. Соболева

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00F82965857DDA33ED257891E9DD8A6331
Владелец: Соболева Ольга Александровна
Действителен: с 01.03.2023 до 24.05.2024

(приказ МОБУ «Муринская СОШ № 6»
от 10.08.2023 № 33)

Положение
об организации и обеспечении информационной безопасности муниципального общеобразовательного бюджетного учреждения «Муринская средняя общеобразовательная школа № 6» (далее - Положение)

Ленинградская область
Всеволожский район
город Мурино
2023 год

I. Общие положения

1.1. Настоящее Положение разработано на основании следующих документов:

- «Конвенция о правах ребенка» (одобрена Генеральной Ассамблеей ООН 20.11.1989) (вступила в силу для СССР 15.09.1990);

- Федеральный закон от 24.07.1998 № 124 «Об основных гарантиях прав ребенка в Российской Федерации»;

- Федеральный закон от 25.07.2002 № 114 «О противодействии экстремисткой деятельности»;

- Федеральный закон от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 29.12.2010 № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию» и все его изменения;

- Федеральный закон от 28.07.2012 № 139 «О защите детей от информации, причиняющей вред их здоровью и развитию»;

- «Концепции информационной безопасности детей в Российской Федерации», утвержденная распоряжением Правительства Российской Федерации от 28.04.2023 № 1105-р;

- Методические рекомендации Совета Федерации Федерального собрания Российской Федерации по ограничению в образовательных организациях, доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

1.2. Настоящее положение разработано с целью ограничения доступа в муниципальном общеобразовательном бюджетном учреждении «Муринская средняя общеобразовательная школа № 6» (далее - Учреждение) к информации, причиняющей вред здоровью и (или) развитию обучающихся, а также не соответствующей целям и задачам образования.

1.3. Контроль организации контентной фильтрации (далее - КФ) ресурсов сети «Интернет» в Учреждении осуществляется Муниципальным учреждением «Всеволожский районный методический центр» (далее - МУ «ВРМЦ»).

1.4. Все обязанности по обеспечению эффективного функционирования средств контентной фильтрации (далее – КФ) регулируются локальными нормативными актами (приказами, положением и должностными инструкциями, утвержденными директором Учреждения).

1.5. Ознакомление с положением и его соблюдение обязательно для всех сотрудников Учреждения.

II. Обязанности работников Учреждения по обеспечению информационной безопасности обучающихся при работе в сети «Интернет»

2.1. Директор Учреждения:

- осуществляет общее управление по организации КФ в Учреждения;

- устанавливает правила по ограничению физического доступа обучающихся к автоматизированным рабочим местам (далее - АРМ) педагогов и сотрудников;

- назначает ответственным за организацию и обеспечение информационной безопасности в Учреждении заместителя директора по безопасности;

- назначает специалиста, ответственного за техническое сопровождение средств КФ ресурсов сети «Интернет»;

- принимает решение о создании совета по обеспечению информационной безопасности обучающихся (далее - Совет) и утверждает его состав;

- контролирует исполнение Плана мероприятий Учреждения по обеспечению информационной безопасности обучающихся при работе в сети «Интернет» на 2023-2024 годы;

- несет полную ответственность за качественное выполнение Плана мероприятий.

2.2. Заместитель директора по безопасности:

- разрабатывает План мероприятий Учреждения по обеспечению информационной безопасности обучающихся при работе в сети «Интернет» (далее - План мероприятий);

- исполняет План мероприятий;

- контролирует деятельность сотрудников Учреждения, в том числе технического специалиста по исполнению Плана мероприятий;

- принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети «Интернет»;

- осуществляет хранение в сейфе логинов и паролей, установленных на операционную систему и программу, осуществляющую КФ на персональных компьютерах обучающихся, и предоставляет их сотрудникам МАУ «ИМЦ» для выполнения функциональных обязанностей.

2.3. Технический специалист:

- исполняет План мероприятий;

- принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательной деятельности.

2.4. Совет по обеспечению информационной безопасности обучающихся:

- принимает участие в реализации Плана мероприятий.

2.5. Сотрудники Учреждения:

- соблюдают в своей профессиональной деятельности законодательство РФ в области информационный безопасности, в том числе КФ при работе с обучающимися в сети «Интернет»;

- исполняют План мероприятий;

- принимают меры по пресечению обращений обучающихся к ресурсам, не имеющим отношения к образовательной деятельности;

III. Работникам Учреждения разрешается:

- отключать средства КФ на своих персональных устройствах, предоставленных педагогическому работнику, только после осуществления образовательной деятельности и отсутствия обучающихся на территории Учреждения, а также получения письменного согласия директора Учреждения, с указанием письменного согласия от директора или заместителя директора по безопасности, с указанием и пояснением целей отключения средств КФ и временных сроках отключения средства КФ с занесением информации в журнал работы КФ.

IV. Работникам Учреждения запрещается:

4.1. При работе на автоматизированном рабочем месте:

1) работать в сети «Интернет», без прохождения соответствующего инструктажа;

2) подключать оборудование, проводить настройку сети и средств КФ (кроме технического специалиста, за техническое сопровождение средств КФ ресурсов сети «Интернет»);

3) отключать СКФ во время нахождения в Учреждении обучающихся;

- использовать поисковые системы Yandex, Google, Rambler, Mail.ru и т.д., кроме поисковых систем сервиса ООО «СкайДНС», http://search.skydns.ru;

4) обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);

5) осуществлять любые сделки через сеть «Интернет»;

6) загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

7) распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы;

8) загружать и распространять:

- материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности компьютерного или телекоммуникационного оборудования;

- программы, для осуществления несанкционированного доступа, серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети «Интернет», а также размещать ссылки на вышеуказанную информацию;

9) пользоваться чужими учетными данными при использовании сетевых сервисов, предполагающих авторизацию.

4.2. Работать на своих персональных (личных) устройствах без СКФ в присутствии обучающихся на территории Учреждения.

V. Заключительные положения

5.1. Все документы об организации и обеспечении информационной безопасности обучающихся при работе в сети «Интернет» в Учреждении должны быть пронумерованы, прошнурованы, скреплены печатью с указанием количества листов и с подписью директора Учреждения.

5.2. Ответственность за ведение документооборота несет заместитель директора по безопасности Учреждения.

5.3. Настоящее Положение является локальным нормативным актом Учреждения, согласовывается с Профсоюзным комитетом и утверждается (либо вводится в действие) приказом директора Учреждения.

5.4. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации.

5.5. Положение принимается на неопределенный срок. Изменения и дополнения к Положению принимаются в порядке, предусмотренном п. 5.3. настоящего Положения.

5.6. После принятия Положения об организации и обеспечении информационной безопасности обучающихся при работе в сети «Интернет» (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция утрачивает силу.