СОГЛАСОВАНО
Общим собранием, Советом обучающихся, Советом родителей (законных представителей) обучающихся Государственного бюджетного профессионального образовательного учреждения (колледжа) города Москвы "Московское хореографическое училище при Московском государственном академическом театре танца "Гжель"
протокол

от "31" августа 2022 года № 1
от "02" сентября 2022 года № 1
от "02" сентября 2022 года № 2

УТВЕРЖДЕНО
приказом Государственного бюджетного профессионального образовательного учреждения (колледжа) города Москвы "Московское хореографическое училище при Московском государственном академическом театре танца "Гжель"

от "02" сентября 2022 года № 77

Положение
об обеспечении информационной безопасности обучающихся и работников Государственного бюджетного профессионального образовательного учреждения (колледжа) города Москвы "Московское хореографическое училище при Московском государственном академическом театре танца "Гжель"

1. Общие положения

1.1. Настоящее Положение об обеспечении информационной безопасности обучающихся и работников Государственного бюджетного профессионального образовательного учреждения (колледжа) города Москвы "Московское хореографическое училище при Московском государственном академическом театре танца "Гжель" (далее – Положение, Учреждение) определяет систему правовых, организационных и технических мероприятий, направленных на обеспечение информационной безопасности обучающихся Учреждения.

1.2. Положение разработано в соответствии с:

– Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646;

– Федеральным законом от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации";

– Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационныхтехнологиях и о защите информации";

– Федеральным законом от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию";

– Федеральным законом от 25.07.2002 № 114-ФЗ "О противодействии экстремистской деятельности";

– Концепцией информационной безопасности детей, утвержденной Распоряжением Правительства Российской Федерации от 02.12.2015 № 2471-р;

– Порядком организации и осуществления образовательной деятельности по основным общеобразовательным программам – образовательным программам начального общего, основного общего и среднего общего образования, утвержденным приказом Министерства образования и науки Российской Федерации от 14.06.2013 № 464;

– Порядком организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования, утвержденным Приказом Министерства просвещения Российской Федерации от 24.08.2022 № 762;

– Порядком применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ, утвержденным приказом Министерства образования и науки Российской Федерации от 23.08.2017 № 816;

– Приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации 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";

– ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения, утверждённым Приказом Ростехрегулирования от 18.12.2008 № 532-ст;

– ГОСТ Р 526532006. Национальный стандарт Российской Федерации. Информационно - коммуникационные технологии в образовании. Термины и определения, утверждённым Приказом Ростехрегулирования от 27.12.2006 № 419-ст;

– ГОСТ Р 53620-2009. Национальный стандарт Российской Федерации. Информационно - коммуникационные технологии в образовании. Электронные образовательные ресурсы. Общие положения, утверждённым Приказом Ростехрегулирования от 15.12.2009№ 956-ст;

– Методическими материалами для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет, направленными Письмом Министерства образования и науки Российской Федерации от 28.04.2014 № ДЛ-115/03;

– 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, направленными Письмом Министерства образования и науки Российской Федерации от 14.05.2018 № 08-1184;

– Уставом Учреждения;

– Политикой информационной безопасности в Учреждении;

– Иными локальными нормативными актами Учреждения.

1.3. Система информационной безопасности является неотъемлемой частью системы комплексной безопасности Учреждения.

1.4. Функционирование системы информационной безопасности в Учреждении обеспечивается применением комплекса правовых, организационных и технических мер защиты, в результате чего снижается или исключается риск, связанный с причинением информационной продукцией, используемой в образовательной деятельности, вреда здоровью и (или) физическому, психическому, духовному, нравственному развитию несовершеннолетних обучающихся.

1.5. Использование сети Интернет в образовательной деятельности допускается только при условии применения административных и организационных мер, технических (программных, программно-аппаратных) средств защиты обучающихся от информации, не совместимой с задачами образования и воспитания, иной информации, распространение которой в Российской Федерации запрещено, информации, причиняющей вред здоровью и (или) развитию детей.

2. Основные цели и задачи функционирования системы информационной безопасности

2.1. Система информационной безопасности направлена защиту единого информационного образовательного пространства Учреждения от незаконного проникновения, на предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в локальных сетях, а также недопущения доступа обучающихся и работников учреждения к информации, которая запрещена или ограничена к распространению в Российской Федерации.

2.2. Система информационной безопасности Школы направлена на решение следующих задач:

– защита прав и законных интересов обучающихся в образовательной деятельности, защита обучающихся от информации, причиняющей вред их здоровью и (или) развитию и (или) не соответствующей задачам образования;

– разграничение объемов и содержания информации, которая может быть

доступна различным категориям пользователей;

– предотвращение утечки, хищения, утраты, подделки информации Учреждения;

– предотвращение несанкционированных действий по уничтожению модификации, искажению, копированию, блокированию информации учреждения;

– предотвращение других форм незаконного вмешательства в информационные ресурсы учреждения и его локальную сеть.

3. Организационно-административные меры, направленные на защиту обучающихся от информации, причиняющей вред их здоровью и (или) развитию

3.1. Приказом по Учреждению назначаются лица, ответственные за обеспечение информационной безопасности. В обязанности ответственных за обеспечение информационной безопасности в том числе входит:

– контроль функционирования системы контентной фильтрации;

– контроль функционирования антивирусной защиты, поддержание в актуальном состоянии антивирусных баз автоматической проверке ПК, локальной сети и внешних носителей на наличие вирусов;

– контроль соблюдения требований по обеспечению информационной безопасности при проведении технического обслуживания и ремонтных работ персональных компьютеров;

– оценка рисков информационной безопасности Учреждения;

– выявление угроз безопасности оборудованию и локальной сети Учреждения;

– проведение инструктажа работников Учреждения по правилам работы с используемыми аппаратно-программными средствами и осуществление контроля за действиями пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования,

– информирование обучающихся, родителей несовершеннолетних обучающихся, работников Учреждения о порядке использования сети Интернет и контроль за использованием сети Интернет обучающимися и работниками.

3.2. В Учреждении разрабатываются и утверждаются локальные нормативные акты, регламентирующие:

– обработку, защиту и хранение персональных данных, права и обязанности обучающихся иработников в сфере защиты персональных данных;

– порядок доступа и использования сети Интернет;

– организацию контроля использования сети Интернет;

– организацию контроля за библиотечным фондом и предотвращение доступа обучающихся к информации экстремистского характера, к информации,

запрещённой
для распространения среди детей и (или) не соответствующей возрасту обучающихся.

3.3. В Учреждении оказывается организационная и методическая поддержка работникам в области безопасной работы с информационными ресурсами, информационными образовательными технологиями, в том числе, путём их направления на повышение квалификации по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети Интернет.

3.4. В Учреждении на регулярной основе осуществляется информирование работников, обучающихся и их родителей (законных представителей) об ответственности за нарушение требований законодательства Российской Федерации, локальных нормативных и организационно- распорядительных актов Учреждения по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети "Интернет".

3.5. В Учреждении разрабатывается, реализуется и совершенствуется комплекс мероприятий, направленный на правовое просвещение обучающихся и родителей (законных представителей) несовершеннолетних обучающихся в сфере информационной безопасности, на формирование навыков обучающихся безопасной работы в информационно- телекоммуникационных сетях.

3.6. Жалобы или претензии о нарушениях законодательства Российской Федерации
о защите детей от информации, причиняющей вред их здоровью и (или) развитию, включая несоответствие применяемых административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, установленным законодательством требованиям, а также о наличии доступа детей к информации, запрещенной для распространения среди детей, и направление мотивированного ответа о результатах рассмотрения таких обращений, жалоб или претензий рассматриваются руководством Учреждения в срок, не превышающий *7* (семи) рабочих дней со дня получения.

3.7. В случае получения обращений, жалоб или претензий о наличии доступа детей
к информации, запрещенной для распространения среди детей, установление причин и условий возникновения такого доступа и принятие мер по их устранению осуществляется руководством Учреждения незамедлительно.

3.8. Мониторинг осуществления организационно - административных мер, направленных на защиту детей от информации, причиняющей вред их здоровью и (или) развитию осуществляется заместителем директора в рамках своих полномочий.

4. Информация, используемая в образовательной деятельности и контроль за ее содержанием

4.1. Информация и (или) информационная продукция, используемая в образовательной деятельности, осуществляемой в учреждении, должна соответствовать требованиям законодательства Российской Федерации к защите детей от информации, причиняющей вред их здоровью и (или) развитию, соответствовать содержанию и задачам образования.

4.2. При осуществлении образовательной деятельности в Учреждении обеспечивается доступ обучающихся и работников к:

– печатной продукции, которая входит в библиотечный фонд Учреждения;

– электронным образовательным ресурсам, прошедшим педагогическую экспертизу, рекомендованным и (или) сформированным органами государственной власти, осуществляющими управление в сфере образования, подведомственными им организациями; разработанными издательствами, выпускающими учебную литературу, учреждениями высшего и среднего образования, российскими библиотеками и иными уполномоченными или допущенными органами и организациями;

– общедоступным государственным и региональным информационным системам;

– информационно-телекоммуникационной сети Интернет в порядке, установленном локальным нормативным актом Учреждения.

4.3. В работе и (или) общении с обучающимися педагогическим работникам или иным работникам Учреждения не допускается использовать информацию:

– направленную на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иную информацию, за распространение которой предусмотрена уголовная или административная ответственность;

– запрещённую для распространения среди детей в соответствии со ст.5 Федерального закона от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровьюи развитию";

- имеющую знак информационной продукции, не соответствующий возрасту обучающегося (обучающихся);

- полученную с нарушением авторских или смежных прав;

- имеющую конфиденциальный характер в соответствии с действующим законодательством и (или) локальными нормативными актами Учреждения.

4.4. Мониторинг содержания информационной продукции, используемой в образовательной деятельности педагогических работников осуществляется

предметными кафедрами, а также администрацией в рамках внутреннего контроля.

4.5. В образовательной и (или) досуговой деятельности с обучающимися, организуемой и проводимой работниками Учреждения, не допускается посещения зрелищных или иных мероприятий, билеты на которые (афиши или иная информация о мероприятии) содержат знак информационной продукции, не соответствующий возрасту обучающегося (обучающихся).

4.6. В Учреждении осуществляется административный контроль за соблюдением возрастной классификации информационной продукции, приобретаемой и (или) используемой в образовательной и (или) досуговой деятельности.

4.7. В процессе осуществления образовательной деятельности с использованием информационно - компьютерных технологий педагогическими работниками осуществляется контроль за использованием обучающимися сети Интернет, в том числе, визуальный контроль.

4.8. При обнаружении угроз информационной безопасности Учреждения, несанкционированного доступа к локальной сети, а также обнаружении доступа к ресурсу, содержание которого может нанести вред здоровью и (или) развитию обучающихся, работники Учреждения обязаны незамедлительно сообщить об этом руководству для принятия соответствующих мер.

4.9. Работники, ответственные за обеспечение информационной безопасности, при получении информации, указанной в п. 4.8. настоящего Положения незамедлительно:

– устанавливают обстоятельства получения доступа к ресурсу сети Интернет, содержащему информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей;

– идентифицируют ресурс сети Интернет;

– в течение 1 (одного) рабочего дня с момента получения информации, указанной в п.4.8. настоящего Положения, проводят мероприятия, направленные на ограничение доступа к ресурсу сети Интернет, содержащему информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей (вносит изменения в политики доступа, применяемые в технических средствах контентной фильтрации, вносят изменения в конфигурацию технических средств контентной фильтрации, в случае необходимости предпринимают другие меры).

– проводят анализ обстоятельств, послуживших причиной доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой

в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей.

– вносят директору Учреждения на основе проведенного анализа предложения
по совершенствованию системы контентной фильтрации в целях минимизации количества инцидентов, связанных с получением доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей.

4.10. В порядке реагирования на инцидент, угрожающий информационной безопасности Учреждения и (или) обучающихся и работников Учреждения, руководством может быть направлено соответствующее сообщение о наличии на страницах сайтов в сети "Интернет" информации, распространение которой в Российской Федерации запрещено в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также в органы внутренних дел.

5. Организационно-технические мероприятия по формированию безопасных условийдоступа обучающихся к ресурсам сети Интернет

5.1. К техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, применяемым при предоставлении доступа к информации, распространяемой посредством сети Интернет, относятся:

- средства ограничения доступа к техническим средствам доступа к сети Интернет;
- средства ограничения доступа к сети Интернет с технических средств третьих лиц;
- средства ограничения доступа к запрещенной для распространения среди детей информации, размещенной на сайтах в сети Интернет.

5.2. В Учреждении обеспечивается антивирусная защита компьютерной техники, систематически проводится обновление антивирусных программ.

5.3. Для приобретения и использования программного обеспечения в образовательной и иной деятельности Учреждения проводится проверка его подлинности.

5.4. В Учреждении с установленной периодичностью осуществляется контроль:

– эксплуатации технических средств контентной фильтрации – постоянно;

– функционирования технических средств контентной фильтрации и их конфигурации – не реже 2 раз в год;

– организации доступа к сети Интернет в целях исключения возможности несанкционированного использования сети Интернет в Учреждении – постоянно;

– функционирования технических средств, применяемых при организации доступа
к сети Интернет, и их конфигурации (компьютерное оборудование, сетевое оборудование, системное и прикладное программное обеспечение) – не реже 2 раз в год;

– изменения конфигурации технических средств, применяемых при организации доступа к сети Интернет, контроль наличия в их составе аппаратных, программных средств, предназначенных для нарушения функционирования технических средств контентной фильтрации – не реже 2 раз в год;

– функционирования системы антивирусной защиты – не реже 1 раза в месяц;

– наличия доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, путем осуществления попыток получения доступа к таким ресурсам сети Интернет – не реже 1 раза в квартал;

5.5. В учреждении не допускается обучающимися и работниками, а также иными лицами самовольная установка программного обеспечения на компьютерную технику Школы, либо использование не принадлежащих Учреждению программ и оборудования.

5.6. Мониторинг осуществления организационно-технических мер, направленных на обеспечение информационной безопасности учреждения осуществляется заместителем директора Учреждения по безопасности в рамках своих полномочий.

6. Обучение и просвещение в сфере информационной безопасности

6.1. В рамках образовательной деятельности в Учреждении осуществляется обучение безопасным способам работы в информационно-телекоммуникационных сетях, в план воспитательной работы Учреждения включаются мероприятия, направленные на повышение медиаграмотности обучающихся, формированию навыков безопасного поведения в сети Интернет.

6.2. В Учреждении проводятся образовательные и консультационные мероприятия
с родителями обучающихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в сеть Интернет.

6.3. На информационных стендах, расположенных в Учреждении и в кабинетах, оснащённых персональными устройствами для выхода в сеть Интернет, размещаются информационные памятки, содержащие основные советы по обеспечению информационной безопасности учащихся.

6.4. На официальном сайте Учреждения размещается специализированный раздел Информационная безопасность, в рамках которого предусмотрено размещение локальных нормативных актов в сфере обеспечения информационной безопасности обучающихся, нормативно-правовых документов, регламентирующих обеспечение информационной безопасности несовершеннолетних, методические рекомендации, информационные памятки для работников, обучающихся и их родителей, направленные на повышение информационной грамотности и обеспечение информационной безопасности детей.

7. Заключительные положения

7.1. Настоящее Положение является локальным нормативным актом Учреждения, согласовывается с Общим собранием работников, Советом обучающихся, Советом родителей (законных представителей) обучающихся Учреждения и утверждается приказом директора Учреждения.

7.2. Настоящее Положение принимается на неопределенный срок.

7.3. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме.

7.4. После принятия настоящего Положения в новой редакции предыдущая редакция автоматически утрачивает силу.