



«УТВЕРЖДАЮ»

Директор ГБОУ Школа № 56  
имени академика В.А. Легасова

Ж.В. Садовникова

«15» сентября 2020 г.

## ПОЛОЖЕНИЕ об информационной безопасности в ГБОУ Школа № 56 имени академика В.А. Легасова

### 1. Общие положения.

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности Государственного бюджетного общеобразовательного учреждения города Москвы «Школа № 56 имени академика В.А. Легасова» (далее – Школа).

1.2. Данное положение разработано в соответствии с Трудовым кодексом 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».

1.3. Под информационной безопасностью Школы следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

Система информационной безопасности Школы направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

1.4. К объектам информационной безопасности в школе относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
- информацию, защита которой предусмотрена законодательными актами РФ в том числе персональные данные;
- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

1.5. Система информационной безопасности Школы должна обязательно обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
- целостность (точность и полноту информации и компьютерных программ);
- доступность (возможность получения пользователями информации в пределах их компетенции).

1.6 Обеспечение информационной безопасности Школы осуществляется по следующим направлениям:

- правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
- инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

### 2. Правовые нормы обеспечения информационной безопасности.

2.1. Школа имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников школы, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.



2.2. Школа обязана обеспечить сохранность конфиденциальной информации.

2.3. Администрация школы:

- назначает ответственного за обеспечение информационной безопасности;
- издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
- имеет право включать требования по обеспечению информационной безопасности в коллективный договор;
- имеет право включать требования по защите информации в договоры по всем видам деятельности;
- разрабатывает перечень сведений конфиденциального характера;
- имеет право требовать защиты интересов школы со стороны государственных и судебных инстанций.

2.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора школы о назначении ответственного за обеспечение информационной безопасности;
- должностные обязанности ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных;
- инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников школы и др.

2.5. Порядок допуска сотрудников школы к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства РФ и школы об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
- инструктаж работника специалистом по информационной безопасности;
- контроль работника ответственного за информационную безопасность при работе с информацией конфиденциального характера.

### **3. Мероприятия по обеспечению информационной безопасности.**

Для обеспечения информационной безопасности в школе требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности школы;
- защита компьютеров, локальных сетей и сети подключения к системе Интернета;
- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся школы;
- учет всех носителей конфиденциальной информации.

### **4. Организация работы с информационными ресурсами и технологиями.**

4.1. Система организации делопроизводства:

- учет всей документации школы, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов школы в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);
- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);
- особый режим уничтожения документов.

4.2. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

4.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

4.2.2. Документы, дела и издания с грифом «Для служебного пользования» («Ограниченного пользования») должны храниться в служебных помещениях в надежно



запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

4.2.3. Выданные для работы дела и документы с грифом «Для служебного пользования» («Ограниченного пользования») подлежат возврату в канцелярию в тот же день.

4.2.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.

4.2.5. Запрещается выносить документы с грифом «Для служебного пользования» за пределы школы.

4.2.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

4.3. Для организации делопроизводства приказом директора школы назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором школы. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

## **5. Обеспечение безопасности в Школьном портале.**

5.1. Школьный портал относится к группе многопользовательских информационных систем с разными правами доступа. С учетом особенностей обрабатываемой информации, система соответствует требованиям, предъявляемым действующим в Российской Федерации законодательством, к информационным системам, осуществляющим обработку персональных данных.

Школьный портал обеспечивает возможность защиты информации от потери и несанкционированного доступа на этапах её передачи и хранения.

Для настройки прав пользователей в системе созданы отдельные роли пользователей с назначением разрешений на выполнение отдельных функций и ограничений по доступу к информации, обрабатываемой в Школьном портале.

5.2. Регламент общих ограничений для участников образовательного процесса при работе со «Школьным порталом», обеспечивающий предоставление Услуги.

5.2.1. Участники образовательного процесса, имеющие доступ к Школьному portalу, не имеют права передавать персональные логины и пароли для входа на Школьный портал другим лицам. Передача персонального логина и пароля для входа в Школьный портал другим лицам влечет за собой ответственность в соответствии с законодательством Российской Федерации о защите персональных данных.

5.2.2. Участники образовательного процесса, имеющие доступ к Школьному portalу, соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль).

5.2.3. Участники образовательного процесса, имеющие доступ к Школьному portalу, в случае нарушения конфиденциальности условий доступа в личный кабинет, уведомляют в течение не более чем одного рабочего дня со дня получения информации о таком нарушении руководителя ОО, службу технической поддержки Школьного портала.

5.2.4. Все операции, произведенные участниками образовательного процесса, имеющими доступ к Школьному portalу, с момента получения информации руководителем ОО и службой технической поддержки о нарушении, указанном в предыдущем абзаце, признаются недействительными.

5.2.5. При проведении работ по обеспечению безопасности информации в Школьном портале участники образовательного процесса, имеющие доступ к Школьному portalу, обязаны соблюдать требования законодательства Российской Федерации в области защиты персональных данных.

## **6. Условия присутствия обучающихся на публичном показе, при публичном исполнении, демонстрации посредством зрелищного мероприятия информационной продукции, запрещенной для детей, в случае их организации и (или) проведения**

6.1. В случае необходимости присутствия детей на публичном показе, при публичном исполнении, демонстрации посредством зрелищного мероприятия информационной продукции, запрещенной для детей, не менее чем за неделю организаторами мероприятия должен быть предоставлен план проведения мероприятия с поминутным регламентом по каждому пункту плана мероприятия.



6.2. Лицо, ответственное за сопровождение детей на данное мероприятие, должно обеспечить организованный вывод детей за 10 минут до демонстрации информационной продукции, запрещенной для детей на расстоянии не менее чем сто метров от границ территорий места проведения зрелищного мероприятия.

**7. Меры защиты детей от информации, причиняющей вред их здоровью и (или) развитию, направленные на повышение осведомленности лиц, находящихся в месте оборота информационной продукции, запрещенной для детей, о необходимости обеспечения информационной безопасности детей и защиты детей от информации, причиняющей вред их здоровью и (или) развитию.**

7.1. Ответственные лица, ответственные за доступ в сети Интернет, устанавливается приказом по школе.

7.2. Ознакомление работников школы, в трудовые обязанности которых входит организация и осуществление оборота информационной продукции, с положениями законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, и настоящим Положением.

7.3. Размещение на информационных стендах и на официальном сайте настоящего положения и локальных актов, регламентирующих работу в сети Интернет и доступ к информации, причиняющей вред здоровью и (или) развитию детей.

7.4. Обеспечение технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и развитию в точках коллективного доступа к сети Интернет осуществляется работниками школы в соответствии с их должностными обязанностями.

7.5. Контроль за соответствием содержания и художественного оформления печатных изданий, полиграфической продукции (в том числе тетрадей, дневников, обложек для книг, закладок для книг), аудиовизуальной продукции, иной информационной продукции, используемой в образовательном процессе требованиям, предъявляемым к информационной продукции для детей соответствующей возрастной группы осуществляется работниками школы в соответствии с их должностными обязанностями и школы и родителями обучающихся в соответствии с их обязанностями, а также с учётом обозначения категории информационной продукции:

- применительно к категории информационной продукции для детей, не достигших возраста шести лет — в виде цифры «0» и знака «плюс»;
- применительно к категории информационной продукции для детей, достигших возраста шести лет — в виде цифры «6» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше шести лет»;
- применительно к категории информационной продукции для детей, достигших возраста двенадцати лет — в виде цифры «12» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше двенадцати лет»;
- применительно к категории информационной продукции для детей, достигших возраста шестнадцати лет — в виде цифры «16» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше шестнадцати лет»;
- применительно к категории информационной продукции, запрещённой для детей, — в виде цифры «18» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «запрещено для детей»;

**8. Процедуры, направленные на предотвращение, выявление и устранение нарушений законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию.**

8.1. Назначение работника, ответственного за применение административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, учитывающих специфику оборота информационной продукции, запрещенной для детей, и за проверку порядка их применения.

8.2. Ознакомление работников школы и обучающихся с Регламентом работы учащихся, учителей и сотрудников школы в Интернет, Правилами использования сети Интернет, Правилами пользования кабинетом свободного доступа, настоящим положением.

8.3. Осуществление контроля за использованием ресурсов сети Интернет во время образовательного процесса.



8.4. Ведение журналов учета работы с ресурсами сети Интернет в точках доступа к сети Интернет для обучающихся.

8.5. Изучение с помощью специальных технических средств контентной фильтрации запрашиваемых адресов Интернет, выявление ресурсов, содержащих информацию, запрещенную законодательством РФ и несовместимую с задачами образования и воспитания.

8.6. Отправка сведений оператору организации, осуществляющей по договору контентную фильтрацию, сведений о выявленных ресурсах, содержащих информацию, запрещенную законодательством РФ, и информацию, несовместимую с задачами образования и воспитания для ограничения доступа к этим ресурсам.

8.7. Рассмотрение в срок, не превышающий десяти рабочих дней со дня получения, обращений, жалоб или претензий о нарушениях законодательства РФ о защите детей от информации, причиняющей вред их здоровью и (или) развитию.

8.8. Установление в течение десяти рабочих дней со дня получения обращений, жалоб или претензий о наличии доступа детей к информации, запрещенной для распространения среди детей, причин и условий возникновения такого доступа и принятие мер по их устранению.

## **9. Рассмотрение обращений, жалоб или претензий о нарушениях законодательства Российской Федерации о защите детей от информации.**

9.1. Обращения, 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, «Требованиям к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию», утвержденных Приказом Минцифры России от 16.06.2014 № 161, а также о наличии доступа детей к информации, запрещенной для распространения среди детей, рассматриваются в срок, не превышающий десяти рабочих дней со дня получения таких обращений, жалоб или претензий. В результате рассмотрения таких обращений, жалоб или претензий направляется мотивированный ответ.

9.2. В течение десяти рабочих дней со дня получения обращений, жалоб или претензий о наличии доступа детей к информации, запрещенной для распространения среди детей, устанавливаются причины и условия возникновения такого доступа, а также принимаются меры по их устранению.