УТВЕРЖДЕНЫ
приказом директора бюджетного учреждения культуры Вологодской области «Вологодский областной театр юного зрителя»
от «01» июня 2022 г. № 66
(приложение № 2 к приказу)

Правила
обработки персональных данных

I. Общие положения

1.1. Данные Правила разработаны с целью защиты интересов бюджетного учреждения культуры Вологодской области «Вологодский областной театр юного зрителя» (далее – Учреждение) и субъектов персональных данных, в целях предотвращения раскрытия (передачи), а также соблюдения надлежащих правил обращения с персональными данными.

1.2. Данные Правила предназначены для использования всеми работниками Учреждения, допущенными к работе с персональными данными.

1.3. Работники Учреждения, доступ которых к персональным данным необходим для выполнения ими своих должностных обязанностей, должны быть ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

II. Порядок работы со сведениями, содержащими персональные данные

2.1. При обработке персональных данных на бумажных носителях, съемных машинных носителях (флеш-носителях, дисках, и т.п.), компьютерах и других технических средствах, работники Учреждения обязаны следить как за сохранностью самих бумажных документов, съемных машинных носителей и компьютеров и других технических средств, так и за сохранностью содержащейся в них информации, а именно не допускать неправомерного ознакомления с ней лиц, не имеющих допуска к работе с персональными данными.

2.2. Запрещается хранение или оставление бумажных документов и съемных машинных носителей, содержащих персональные данные, в виде, позволяющем осуществить визуальный просмотр содержащихся в них персональных данных, их фотографирование или несанкционированное создание копий.

2.3. Напечатанные документы, содержащие персональные данные, должны изыматься из принтеров немедленно.

Хранение бумажных документов и съемных машинных носителей, содержащих персональные данные, допускается только в помещениях, к которым исключен доступ лиц, не допущенных к обработке соответствующих персональных данных.

2.4. Запрещается без прямой служебной необходимости делать выписки персональных данных, распечатывать документы с персональными данными или записывать персональные данные на съемные машинные носители.

2.5. Запрещается выносить документы, съемные машинные носители или переносные компьютеры, содержащие персональные данные, за пределы помещений контролируемой зоны Учреждения, если это не требуется для выполнения трудовых обязанностей и если на это не дано разрешение директора Учреждения или ответственного за организацию обработки персональных данных.

2.6. Бумажные документы с персональными данными, у которых истек срок хранения, лишние или испорченные копии документов с персональными данными, должны быть уничтожены без возможности их восстановления.

2.7. Большие объемы бумажных документов с персональными данными, съемные машинные носители с персональными данными, а также встроенные в компьютеры носители с персональными данными должны уничтожаться под контролем ответственного за организацию обработки персональных данных, способом, исключающим дальнейшее восстановление информации.

2.8. Мониторы компьютеров, использующихся для обработки персональных данных, должны быть ориентированы таким образом, чтобы исключить визуальный просмотр информации с них лицами, не имеющими допуск к обработке персональных данных.

2.9. Запрещается установка и использование при работе на автоматизированных рабочих местах вредоносных программ, ведущих к блокированию работы сети, самовольное изменение сетевых адресов, самовольное вскрытие блоков автоматизированных рабочих мест, модернизация или модификация автоматизированных рабочих мест и программного обеспечения, а также несанкционированная передача автоматизированных рабочих мест с прописанными сетевыми настройками. Передача автоматизированных рабочих мест из одного структурного подразделения в другое производится только ответственным за обеспечение безопасности информации с предварительно удаленными сетевыми настройками.

2.10. Для работы с персональными данными разрешается использовать только автоматизированные рабочие места, указанные в Перечне автоматизированных рабочих мест информационных систем.

2.11. Запрещается упоминать в разговоре с третьими лицами сведения, содержащие персональные данные.

2.12. Запрещается в нерабочее время или за пределами помещений Учреждения упоминать в разговоре с кем-либо, включая любых работников Учреждения, сведения, содержащие персональные данные.

2.13. Запрещается обсуждать порядок доступа, места хранения, средства и методы защиты персональных данных с кем-либо, кроме ответственного за организацию обработки персональных данных, ответственного за обеспечение безопасности персональных данных в информационных системах, руководства, или лица, уполномоченного руководством на обсуждение данных вопросов.

III. Порядок доступа лиц в помещения

3.1. При обеспечении доступа лиц соблюдаются требования законодательства Российской Федерации по защите персональных данных.

3.2. Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности структурных подразделений, и определяет порядок пропуска работников Учреждения и иных третьих лиц в помещения.

3.3. Контроль за порядком обеспечения доступа лиц в помещения возлагается на руководителей структурных подразделений.

3.4. Не допускается нахождение работников Учреждения в помещениях контролируемой зоны в нерабочее для них время без согласования с руководством.

3.5. В случаях, не терпящих отлагательства (пожар, авария систем тепло-, водоснабжения и т.п.), когда находящимся в помещении оборудованию, материальным ценностям и документации грозит опасность уничтожения или вывода из строя, работник оповещает пожарную охрану (аварийную службу), вызывает руководителя подразделения или работника, ответственного за помещение. Помещение вскрывается до прибытия указанных лиц, и принимаются меры к тушению пожара (ликвидации аварии), эвакуации ценностей, имущества и документации.

Около эвакуируемых ценностей, имущества и документации выставляется временный пост охраны. Акт о вскрытии помещения составляется после окончания работ, связанных с ликвидацией происшествия.

3.6. Нахождение посетителей допускается только в рабочее время в присутствии работников, имеющих допуск к персональным данным.

3.7. В помещения, в которых используются информационные системы персональных данных, пропускаются:

3.7.1. беспрепятственно – директор Учреждения и работники, имеющие допуск к работе с персональными данными и с целью выполнения должностных обязанностей;

3.7.2. при наличии служебного удостоверения, с разрешения директора Учреждения или руководителя структурного подразделения, в сопровождении ответственного за организацию обработки персональных данных или руководителя

структурного подразделения – работники контролирующих органов, работники пожарных и аварийных служб, работники полиции;

3.7.3. ограниченно – работники, не имеющие допуска к работе с персональными данными или не имеющие функциональных обязанностей в помещении, работники сторонних организаций и учреждений для выполнения договорных отношений.

3.8. Посетители пропускаются в помещения Учреждения, в которых используются информационные системы персональных данных, в рабочее время в сопровождении работников, допущенных к обработке персональных данных.

3.9. В помещениях, в которых происходит обработка персональных данных, запрещено использование не предусмотренных должностными обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

3.10. Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных директором Учреждения или руководителями структурных подразделений Учреждения.

3.11. В целях предотвращения несанкционированного доступа к сведениям, содержащим персональные данные, работы проводятся только под контролем ответственного за организацию обработки персональных данных или руководителя структурного подразделения.

3.12. Контроль за допуском в помещения контролируемой зоны в рабочее время возлагается на руководителей подразделений, за которыми закреплены данные помещения. В нерабочее время, выходные и нерабочие праздничные дни охрана помещений контролируемой зоны обеспечивается средствами охранной сигнализации, а в случае их неисправности выставлением поста охраны.

3.13. Для исключения возможности бесконтрольного проникновения в помещения и к установленному в них оборудованию посторонних лиц, двери в отсутствие штатных работников запираются на ключ.

3.14. Оборудование в помещении должно размещаться таким образом, чтобы исключить возможность бесконтрольного доступа к нему посторонних лиц.

3.15. Окна помещений, в которых ведется обработка персональных данных, должны быть оборудованы шторами или жалюзи.

3.16. Уборка помещений, в которых используются информационные системы персональных данных, должна производиться под контролем работника, допущенного к обработке персональных данных в этом помещении.

3.17. Во время уборки в помещении должна быть приостановлена работа с персональными данными, должны быть выключены или заблокированы все автоматизированные рабочие места, на которых обрабатываются персональные данные. Носители, содержащие персональные данные, должны быть убраны в шкафы или сейфы.

IV. Действия при обнаружении попыток несанкционированного доступа

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

4.1.2. действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к информационной системе персональных данных при использовании учетной записи администратора или другого пользователя информационной системы персональных данных, методом подбора пароля, использования личного пароля, разглашенного владельцем учетной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа пользователь информационной системы персональных данных обязан:

4.2.1. прекратить несанкционированный доступ к персональным данным;

4.2.2. доложить директору Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

4.2.4. известить ответственного за обеспечение безопасности персональных данных в информационных системах и ответственного за организацию обработки персональных данных о факте несанкционированного доступа.

V. Требования по техническому укреплению

5.1. Руководители структурных подразделений обеспечивают обязательное выполнение мероприятий по техническому укреплению и оборудованию специальными техническими средствами охраны, системами пожарной безопасности и должны руководствоваться следующими основными требованиями:

5.1.1. Двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек.

5.1.2. Конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол.

5.1.3. Стекла в рамах должны быть надежно закреплены в пазах.

5.1.4. Рамы указанных оконных проемов должны оборудоваться запорными устройствами.