Приложение 7
к приказу МАУДО «ДПШ»
от 31.08.2020 № 276/1-од

Правила
обработки персональных данных

I. Общие положения

1. Данные Правила разработаны с целью защиты интересов Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска» (далее - МАУДО «ДПШ») и субъектов персональных данных, в целях предотвращения раскрытия (передачи), а также соблюдения надлежащих правил обращения с персональными данными.

2. Данные Правила предназначены для использования всеми работниками МАУДО «ДПШ», допущенными к работе с персональными данными.

3. Работники МАУДО «ДПШ», доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей, должны быть ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных

II. Термины и определения

4. **Информация** - сведения (сообщения, данные) независимо от формы их представления (ст.2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»).

Доступ к информации – возможность получения информации и её использования (ст.2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»).

Носитель информации - любой материальный объект или среда, используемый для хранения или передачи информации.

Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т.д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т.д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

Информационная система (ИС) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т.д.), которые обеспечивают и распространяют информацию.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Пароль – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Субъект персональных данных — физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

III. Порядок работы со сведениями, содержащими персональные данные

5. При обработке персональных данных на бумажных носителях, съёмных носителях (дискетах, дисках, флеш-носителях и т.п.), компьютерах и других технических средствах, работники МАУДО «ДПШ» обязаны следить как за сохранностью самих бумажных документов, съёмных 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.

6. Запрещается хранение или оставление бумажных документов и съёмных носителей, содержащих персональные данные, в виде, позволяющем осуществить визуальный просмотр содержащихся в них персональных данных, их фотографирование или несанкционированное создание копий. Напечатанные документы, содержащие персональные данные, должны изыматься из принтеров немедленно. Хранение бумажных документов и съёмных носителей, содержащих персональные данные, допускается только в специальных закрытых шкафах,

сейфах и помещениях, к которым исключён доступ лиц, не допущенных к обработке соответствующих персональных данных.

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

8. Запрещается использовать для передачи персональных данных съёмные носители, не учтённые в «Журнале учета съемных носителей информации».

9. Запрещается выносить документы, съёмные носители или переносные компьютеры, содержащие персональные данные, за пределы служебных помещений МАУДО «ДПШ», если это не требуется для выполнения служебных (трудовых) обязанностей и если на это не дано разрешение директора МАУДО «ДПШ» или ответственного за организацию обработки персональных данных.

10. Бумажные документы с персональными данными, у которых истёк срок хранения, лишние или испорченные копии документов с персональными данными, должны быть уничтожены без возможности их восстановления (например, в шредерах).

11. Большие объёмы бумажных документов с персональными данными, съёмные 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.

12. 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.

13. Запрещается установка и использование при работе в АРМ вредоносных программ, ведущих к блокированию работы сети, самовольное изменение сетевых адресов, самовольное вскрытие блоков АРМ, модернизация или модификация АРМ и программного обеспечения. Несанкционированная передача АРМ с прописанными сетевыми настройками. Передача АРМ из одного подразделения в другое производится только ответственным за обеспечение безопасности информации с предварительно удаленными сетевыми настройками. Использование технологии беспроводного доступа без разрешения ответственного за обеспечение безопасности в информационных системах.

14. Для работы с персональными данными разрешается использовать только автоматизированные рабочие места, указанные в «Перечне автоматизированных рабочих мест информационных систем», при этом для обработки персональных данных можно использовать только программное обеспечение, указанное в «Перечне общесистемного и прикладного программного обеспечения».

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

16. Запрещается в нерабочее время или за пределами служебных помещений упоминать в разговоре с кем-либо, включая любых работников МАУДО «ДПШ», сведения, содержащие персональные данные.

17. 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.

IV. Порядок доступа лиц в помещения

18. При обеспечении доступа лиц соблюдаются требования законодательства РФ по защите персональных данных.

19. Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности структурных подразделений и определяет порядок пропуска работников МАУДО «ДПШ» и иных третьих лиц в помещения.

20. Контроль за порядком обеспечения доступа лиц в помещения возлагается на руководителя структурного подразделения.

21. Не допускается нахождение работников МАУДО «ДПШ» в помещениях в нерабочее для них время без согласования с руководством и без служебной записки. В нерабочее время, в случае служебной необходимости могут задержаться на рабочих местах только при наличии служебной записки, подписанной руководителем структурного подразделения. В служебной записке указывается (Ф.И.О. работника, № кабинета и время окончания работы, при работе нескольких человек указывается ответственное лицо). Служебная записка предоставляется ответственному за организацию обработки персональных данных. В случае неотложных заданий, поступивших после окончания рабочего дня, порядок допуска в служебные помещения осуществляется аналогичным образом, по личному разрешению ответственного за организацию обработки персональных данных до начала неотложных работ.

22. 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. Служебное 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.

23. Нахождение посетителей допускается только в рабочее время в присутствии работников имеющих допуск.

24. В помещения ИС пропускаются:

- беспрепятственно – директор МАУДО «ДПШ» и работники, имеющие допуск к работе с персональными данными и с целью выполнения должностных обязанностей;

- при наличии служебного удостоверения, с разрешения директора МАУДО «ДПШ» 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;

- 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.

25. Посетители пропускаются в помещения ИС МАУДО «ДПШ» в рабочее время в сопровождении работников, допущенных к обработке персональных данных.

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

27. Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных руководством МАУДО «ДПШ».

28. 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.

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

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

31. Помещения, где хранятся персональные данные, защищаемые криптографическими средствами защиты информации, должны быть оснащены входными дверьми с замками для обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода. Помещения должны опечатываться по окончании рабочего дня или быть

оборудованы соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

32. Руководители структурных подразделений, либо работники, уполномоченные хранить ключи от сейфов и помещений, должны вести «Журнал учета ключей от сейфов и помещений».

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

34. Окна помещений, в которых ведётся обработка персональных данных, должны быть оборудованы шторами или жалюзи.

35. Режим работы охраны устанавливается штатным расписанием и должностными инструкциями.

36. Уборка помещений ИС должна производиться под контролем работника, допущенного к обработке персональных данных в этом помещении.

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

V. Действия при обнаружении попыток несанкционированного доступа

38. К попыткам несанкционированного доступа относятся:

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

- действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИС, при использовании учётной записи администратора или другого пользователя ИС, методом подбора пароля, использования личного пароля, разглашённого владельцем учётной записи или любым другим методом.

39. При выявлении факта несанкционированного доступа пользователь ИСПДн обязан:

1) прекратить несанкционированный доступ к персональным данным;

2) доложить директору МАУДО «ДПШ» служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

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

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

VI. Требования по техническому укреплению

40. 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:

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;

2) оконные проемы первых этажей зданий должны быть укреплены металлическими решетками, запираемыми с внутренней стороны, если это не противоречит требованиям пожарной безопасности;

3) конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол;

4) стекла в рамах должны быть надежно закреплены в пазах;

5) рамы указанных оконных проемов должны оборудоваться запорными устройствами.

VII. Ответственность

41. Работники МАУДО «ДПШ», виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

42. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) МАУДО «ДПШ», влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник МАУДО «ДПШ», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба МАУДО «ДПШ» (в соответствии с п.7 ст.243 Трудового кодекса РФ).

В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст.13.14 Кодекса об административных правонарушениях РФ.

43. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст.137 Уголовного кодекса РФ.

44. Директор МАУДО «ДПШ» за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст.5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.