

ИНСТРУКЦИЯ

О порядке работы с персональными данными работников Муниципального бюджетного учреждения дополнительного образования Спортивная школа олимпийского резерва № 1 по конькобежному спорту города Челябинска

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Инструкция о порядке работы с персональными данными (далее – Инструкция) работников Муниципального бюджетного учреждения дополнительного образования Спортивная школа олимпийского резерва №1 по конькобежному спорту города Челябинска (далее - Учреждение) разработана с целью защиты интересов субъектов персональных данных, в целях предотвращения раскрытия (передачи), а также соблюдения надлежащих правил обращения с персональными данными.
2. Данная Инструкция предназначена для использования всеми допущенными к работе с персональными данными сотрудниками Учреждения.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- Информация – сведения (сообщения, данные) независимо от формы их представления.
- Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.
- Доступ к информации – возможность получения информации и ее использования.
- Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.
- Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
- Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
- 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.
- Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
- 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.

3. ПОРЯДОК РАБОТЫ СО СВЕДЕНИЯМИ, СОДЕРЖАЩИМИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

3. При обработке персональных данных на бумажных документах, съемных носителях, компьютерах и других технических средствах, сотрудники Учреждения обязаны следить как за сохранностью самих бумажных документов, съемных 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 доступа к работе с персональными данными.
4. Запрещается хранение или оставление бумажных документов и съемных 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 съемных носителей, содержащих персональные данные, допускаются только в специальных закрытых шкафах и сейфах, к которым исключен доступ лиц, не допущенных к обработке соответствующих персональных данных.
5. Запрещается без прямой служебной необходимости делать выписки персональных данных, распечатывать документы с персональными данными или записывать персональные данные на съемные носители.
6. Запрещается выносить документы, съемные носители или переносные компьютеры, содержащие персональные данные, за пределы служебных помещений, если это не требуется для выполнения трудовых обязанностей, и если на это не дано разрешение ответственного за организацию обработки персональных данных.
7. 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.
8. Большие объемы бумажных документов с персональными данными, съемные 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.
9. Мониторы компьютеров, используемых для обработки персональных данных, должны быть ориентированы таким образом, чтобы исключить визуальный просмотр информации с них лицами, не имеющими допуск к обработке персональных данных.
10. Категорически запрещается упоминать в разговоре с третьими лицами сведения, содержащие персональные данные.
11. Запрещается в нерабочее время или за пределами служебных помещений упоминать в разговоре с кем-либо, включая любых сотрудников Учреждения, сведения, содержащие сведения.
12. Запрещается обсуждать порядок доступа, места хранения, средства и методы защиты персональных данных с кем-либо, кроме ответственного за организацию обработки

персональных данных, руководства или лица, уполномоченного руководством на обсуждение данных вопросов.

4. ПОРЯДОК ДОСТУПА ЛИЦ В ПОМЕЩЕНИЯ

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

14. Контроль за порядком обеспечения доступа лиц в помещения возлагается на директора Учреждения.

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

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

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

18. Уборка помещений должна производиться под контролем сотрудника, допущенного к обработке персональных данных в этом помещении. Во время уборки в помещении должна быть приостановлена работа с персональными данными, должны быть выключены или заблокированы все АРМ, а которых обрабатываются персональные данные. Носители содержащие персональные данные, должны быть убраны в закрытый шкаф или сейф.

5. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

19. Сотрудники Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством РФ.

20. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним доступ), 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), влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник Учреждения, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Учреждению. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии с Кодексом об административных правонарушениях. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии с Уголовным кодексом РФ.