

**ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
СОТРУДНИКОВ**

Муниципального бюджетного учреждения
дополнительного образования
«Центр внешкольной работы имени С.А. Криворотовой»

СОГЛАСОВАНО

С общим собранием трудового коллектива
Протокол № 2
от « 26 » 08. 2015 г.

УТВЕРЖДЕНО

Приказом директора
МБУ ДО ЦВР № 79
от « 03 » 09. 2015 г.

I. Общие положения

1. Цель Положения - защита персональных данных работников МБУ ДО ЦВР от несанкционированного доступа.
2. Сбор, хранение, использование и распространение информации о частной жизни лица без письменного его согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации.
3. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, если иное не определено законом.
4. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.
5. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении; о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.
6. Юридические и физические лица, в соответствии со своими полномочиями, владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.
7. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов, действующих на основании статей 14 и 15 Федерального закона и Законодательства о персональных данных.
8. Настоящее Положение утверждается приказом директора МБУ ДО ЦВР и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным сотрудника.

II. Понятие и состав персональных данных

9. Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника.
10. Состав персональных данных работника:
 - анкетные и биографические данные;
 - образование;

- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность,
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики.

Данные документы являются конфиденциальными, учитывая их массовость и единое место обработки и хранения – соответствующий гриф ограничения на них не ставится.

III. Обязанности работодателя

11. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

- обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

- при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными федеральными законами.

- при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных

исключительно в результате их автоматизированной обработки или электронного получения.

- защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

- работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

12. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

IV. Обязанности работника

13. Работник обязан передавать работодателю или его полномочному должностному лицу комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ.

14. Работник обязан своевременно сообщать работодателю об изменении своих персональных данных.

V. Права работника

15. Работник может требовать исключения или исправления неверных или неполных персональных данных.

16. Работник имеет право на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные.

17. Работник имеет право дополнять персональные данные оценочного характера заявлением, выражающим его собственную точку зрения.

18. Работник имеет право определять своих представителей для защиты своих персональных данных.

19. Работник имеет право на сохранение и защиту своей личной и семейной тайны.

VI. Сбор, обработка и хранение персональных данных

20. Обработка персональных данных работника – это получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

21. Порядок получения персональных данных.

- все персональные данные работника следует получать у него самого. Если персональные данные возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

- работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ, работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

- работодатель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

22. К обработке, передаче и хранению персональных данных работника могут иметь доступ:

- члены администрации;
- сотрудники бухгалтерии;
- секретарь;
- руководители методических объединений.

23. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья, а также в случаях, установленных Федеральным законом;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности);

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать

только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям, имеющим отношение к обработке, передаче и хранению персональных данных в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

24. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

25. При передаче персональных данных работника потребителям за пределы образовательного учреждения, работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных Федеральным законом.

26. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

27. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

28. По возможности персональные данные обезличиваются.

VIII. Доступ к персональным данным сотрудника

29. Внутренний доступ.

Право доступа к персональным данным сотрудника имеют:

- директор МБУ ДО ЦВР;
- заместитель директора учреждения;
- секретарь;
- руководители методических объединений;
- работники бухгалтерии Центра;
- сам работник, носитель данных.

Другие сотрудники учреждения имеют доступ к персональным данным работника только с письменного согласия самого работника, носителя данных.

30. Внешний доступ.

К числу массовых потребителей персональных данных вне образовательного учреждения относятся государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления;
- организация здравоохранения при прохождении ежегодного медицинского осмотра.

31. Надзорно - контрольные органы имеют доступ к информации только в сфере своей компетенции.

32. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

33. Другие организации. Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

34. Родственники и члены семей. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника. В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия. (УК РФ).

VIII. Защита персональных данных

35. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и

линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности учреждения.

36. «Внутренняя защита».

Для защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;

- строгое избирательное и обоснованное распределение документов и информации между работниками;

- знание работником требований нормативно – методических документов по защите информации и сохранении тайны;

- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

- организация порядка уничтожения информации;

- своевременное выявление нарушения требований разрешительной системы доступа;

- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

37. Защита персональных данных сотрудника на электронных носителях.

Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается директору образовательного учреждения.

38. «Внешняя защита».

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности МБУ ДО ЦВР, посетители, работники других организационных структур.

39. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:
- пропускной режим Центра;
 - порядок охраны территории, зданий, помещений;
 - требования к защите информации при интервьюировании и собеседованиях.
40. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с Федеральными законами.

IX. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

41. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.
42. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.
43. Каждый сотрудник образовательного учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.
44. Лица, виновные в нарушении установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных), несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законом.

Принято с учетом мнения:

общего собрания трудового коллектива протокол № 2 от «26» 08. 2015 г.