Приложение №2
к приказу №____ от «__» _____ 2022 г.

Положение о защищаемой информации

1. Общие положения

1.1. Настоящее Положение о защищаемой информации (далее - Положение):

а) Является основополагающим внутренним документом КГБОУ ШИ 12 (далее – Учреждение), регулирующим вопросы и правила обработки защищаемой информации, в том числе персональных данных (далее - ПДн), в информационной системах (далее – ИС) Учреждения;

б) Устанавливает процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере защиты информации;

в) Определяет содержание защищаемой информации, а также цели ее обработки.

1.2. Настоящее Положение разработано в соответствии со следующими нормативно-правовыми актами РФ:

а) Конституция Российской Федерации (от 25.12.1993);

б) Федеральный закон «Об информации, Информационных технологиях и о защите информации» (№ 149- ФЗ от 27.07.2006);

в) Федеральный закон «О персональных данных» (№ 152-ФЗ от 27.07.2006);

г) Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (№ 1119 от 01.11.2012);

д) Постановление Правительства РФ «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (№ 687 от 15.09.2008);

е) Постановление Правительства РФ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися

государственными или муниципальными органами» (№ 211 от 21.03.2012);

ж) Иные нормативно-правовые акты, разработанные в соответствии с федеральным законом «О персональных данных».

1.3. ПДн относятся к категории конфиденциальной информации.

1.4. Учреждение обрабатывает следующие категории защищаемой информации:

а) Персональные данные физических лиц, работающих по трудовому договору с Учреждением (далее - Работники);

б) Персональные данные физических лиц, являющихся стороной договора гражданско-правового характера (далее - Контрагенты);

в) Персональные данные обучающихся, воспитанников в Учреждении (далее - Ученики);

г) Персональные данные родителей (законных представителей) Учеников (далее - Родители).

д) Персональные данные участников системы электронного документооборота Правительства Хабаровского края (далее – СЭД).

1.5. Учреждение осуществляет обработку ПДн Работников исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

1.6. Учреждение осуществляет обработку ПДн Контрагентов исключительно в целях исполнения договора гражданско-правового характера.

1.7. Учреждение осуществляет обработку ПДн Учеников и Родителей исключительно в целях реализации в полной мере основных общеобразовательных программ начального общего, основного общего образования по адаптированным основным общеобразовательным программам, реализации основных программ профессионального обучения и реализации дополнительных общеобразовательных программ.

1.8. Учреждение обрабатывает ПДн участников СЭД, необходимые для осуществления возможностей по организации безбумажного документооборота в пределах органов исполнительной власти Хабаровского края.

1.9. Настоящее Положение вступает в силу на основании приказа директора КГБОУ ШИ 12.

1.10. Все изменения в Положение вносятся приказом директора КГБОУ ШИ 12.

2. Основные термины и понятия

2.1. Основные термины и понятия, указанные в п. 2 настоящего положения используются в иных локальных документах Учреждения, принимаемых по вопросу обработки защищаемой информации в ИС Учреждения.

2.2. Для целей настоящего положения используются следующие термины и понятия:

а) Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

б) Субъект - субъект персональных данных;

в) 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.

2.3. Персональные данные Работников - информация, необходимая Учреждению для обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.4. Персональные данные Контрагентов - информация, необходимая Учреждению для исполнения договора гражданско-правового характера.

2.5. Персональные данные физических лиц участников СЭД - информация, необходимая для осуществления возможностей по организации безбумажного документооборота в системе электронного документооборота Правительства Хабаровского края.

2.6. Персональные данные Учеников и Родителей – информация, необходимая для реализации в полной мере основных общеобразовательных программ начального общего, основного общего образования по адаптированным основным общеобразовательным программам, реализации основных программ профессионального обучения и реализации дополнительных общеобразовательных программ.

3. Общие правила обработки защищаемой информации

3.1. В Учреждении устанавливаются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере защиты информации, в том числе персональных данных.

3.2. К обработке защищаемой информации допускаются только штатные работники, внесенные в список лиц, допущенных к обработке защищаемой информации и соответствующие должности, внесенной в перечень должностей работников, допущенных к обработке защищаемой информации.

3.3. При работе с защищаемой информацией, в том числе при обработке персональных данных в ИС Учреждения, работники, допущенные к обработке защищаемой информации, руководствуются инструкцией пользователя ИС Учреждения.

3.4. Приказом директора КГБОУ ШИ 12 для ИС Учреждения назначается лицо, ответственное за организацию обработки персональных данных.

3.5. Лицо, ответственное за организацию обработки персональных данных, в своей деятельности руководствуется инструкцией лица, ответственного за организацию обработки персональных данных.

3.6. Лицом ответственным за организацию обработки персональных данных определяется список лиц, допущенных в помещения, в которых производится обработка защищаемой информации.

3.7. Лицом, ответственным за организацию обработки персональных данных, производится учет обращений субъектов персональных данных или их законных представителей.

3.8. Каждое лицо, допущенное к обработке защищаемой информации, обязуется не разглашать информацию конфиденциального характера, в том числе персональные данные, полученные в результате исполнения своих должностных обязанностей.

3.9. Все места хранилищ носителей информации должны быть учтены.

3.10. Все нормативные акты, указанные в п. 3.1-3.7 вступают в силу с момента их утверждения директором КГБОУ «Школа-интернат №12» и действуют бессрочно до замены их новыми актами.

4. Правила обработки защищаемой информации в ИС Учреждения

4.1. В Учреждении устанавливаются и соблюдаются процедуры, направленные на выявление и предотвращение нарушений законодательства

Российской Федерации в сфере защиты информации, в том числе персональных данных, обрабатываемых в ИС Учреждения.

4.2. Приказом директора КГБОУ ШИ 12 утверждается перечень информационных систем Учреждения.

4.3. Определение необходимого уровня защищенности ИС осуществляется комиссией, утвержденной приказом директора КГБОУ ШИ 12. В комиссию должны входить не менее трех человек из числа Работников Учреждения. По завершении процедуры классификации составляется Акт определения требуемого уровня защищенности ИС.

4.4. Состав персональных данных, обрабатываемых в ИС Учреждения, а также цели их обработки определяются в перечне защищаемой информации.

4.5. Для ИС приказом директора КГБОУ ШИ 12 назначается администратор информационной безопасности (далее – Администратор).

4.6. Администратор в своей деятельности руководствуется инструкцией администратора информационной безопасности.

4.7. К техническому обслуживанию средств и систем ИС Учреждения допускаются только лица, внесенные в список лиц, допущенных к техническому и программному обслуживанию ИС Учреждения.

4.8. К управлению конфигурацией ИС Учреждения и системы защиты информации допускаются только лица, внесенные в список лиц, допущенных к управлению конфигурацией ИС и системы защиты информации.

4.9. Любые изменения в конфигурации ИС Учреждения, влияющие на защищенность конфиденциальной информации, обрабатываемой в ИС Учреждения, должны быть учтены Администратором в журнале регистрации изменений в конфигурации ИС Учреждения.

4.10. Администратор в согласовании с лицом, ответственным за организацию обработки персональных данных, составляет технический паспорт ИС Учреждения.

4.11. Для предотвращения возможных потерь информации с носителей, содержащих защищаемую информацию, Администратором разрабатывается инструкция по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

4.12. Для защиты автоматизированных рабочих мест (далее – АРМ) лиц, допущенных к обработке защищаемой информации, от вирусов и шпионских программ, Администратором разрабатывается инструкция по организации антивирусной защиты.

4.13. Для защиты автоматизированных рабочих мест лиц, производящих обработку защищаемой информации от несанкционированного

доступа, Администратором разрабатывается инструкция по организации парольной защиты.

4.14. Все съемные и машинные носители защищаемой информации подлежат учету. Администратором разрабатывается инструкция по порядку учета и хранения машинных и съемных носителей информации.

4.15. В случае если в информационной системе имеется разграничение прав доступа пользователей к защищаемой информации, Администратор разрабатывает разрешительную систему доступа к информационным ресурсам.

4.16. Приказом директора КГБОУ ШИ 12 утверждается перечень регистрируемых событий безопасности. Администратор обеспечивает сбор, обработку, хранение и конфиденциальность таких событий.

4.17. Для определения вероятных нарушителей и актуальных угроз безопасности в ИС Учреждения Администратором оператора разрабатывается модель угроз безопасности ИС Учреждения.

4.18. Ежегодно, не позднее 15 августа комиссия, указанная в п.4.3 разрабатывает план мероприятий по обеспечению защиты информации на период с 01 сентября текущего года по 31 августа следующего года. Утвержденный план учитывать при разработке мероприятий на учебный год.

4.19. Лицо, ответственное за организацию обработки персональных данных производит учет всех мероприятий, направленных на обеспечение безопасности защищаемой информации, обрабатываемой в Учреждении в журнале учета мероприятий по защите информации.

4.20. Все субъекты персональных данных, данные которых обрабатываются в ИС, подтверждают свое согласие на обработку персональных данных в письменном виде.

4.21. Лицо, ответственное за организацию обработки персональных данных направляет и поддерживает в актуальном состоянии уведомление об обработке персональных данных в Управлении Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Хабаровскому краю и Еврейской автономной области.

4.22. Все нормативные акты, указанные в п. 4.1-4.21 вступают в силу с момента их утверждения директором КГБОУ ШИ 12 и действуют бессрочно до замены их новыми актами.

4.23. Не допускается обработка защищаемой информации в ИС Учреждения:

а) При отсутствии установленных и настроенных сертифицированных средств защиты информации;

б) При отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы.

4.24. При обработке защищаемой информации запрещается:

а) Обрабатывать защищаемую информацию в присутствии лиц, не допущенных к их обработке;

б) Осуществлять ввод информации под диктовку.

5. Правила обработки защищаемой информации без использования средств автоматизации

5.1. Обработка защищаемой информации без использования средств автоматизации (далее - неавтоматизированная обработка информации) может осуществляться в виде документов на бумажных носителях.

5.2. При неавтоматизированной обработке информации:

а) Не допускается фиксация на одном бумажном носителе информации, цели, обработки которой заведомо не совместимы;

б) Персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

в) Документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

г) Дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

5.3. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание)

5.4. Факт уничтожения носителей защищаемой информации оформляется внутренним актом, в котором указывается какая информация, когда, кем и каким образом уничтожены.

6. Правила обработки защищаемой информации с применением средств криптографической защиты информации

6.1. Двери помещений, где размещены средства криптографической защиты информации (далее - СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее - Помещения) должны быть оснащены замками.

6.2. Двери Помещений должны быть постоянно закрыты на замок, за исключением необходимости санкционированного прохода.

6.3. Двери Помещений должны опечатываться по окончанию рабочего дня или оборудоваться соответствующим техническим устройством, сигнализирующем о несанкционированном вскрытии.

6.4. Администратором разрабатываются правила доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях.

6.5. Все пользователи, применяющие СКЗИ для обработки защищаемой информации в ИС Учреждения, должны быть ознакомлены с инструкцией по работе с СКЗИ, сертификатами ключей подписи, открытыми и закрытыми ключами электронной цифровой подписи.

6.6. К работе с СКЗИ допускаются только лица, внесенные в список лиц, допущенных к работе СКЗИ.

6.7. Перед внесением пользователя ИС Учреждения в списки лиц, допущенных к работе с СКЗИ, Администратор проводит инструктаж по работе с СКЗИ с записью в журнал учета проведения инструктажа пользователя, допущенного к работе с СКЗИ.

6.8. Администратор обязан вести учет всех СКЗИ, эксплуатационной и технической документации к ним и ключевых документов, используемых в ИС Учреждения.

6.9. Администратор обязан вести учет носителей с ключевой информацией.

7. Ответственность за нарушение норм, регулирующих обработку и защиту информации

7.1. Лицо, ответственное за организацию обработки персональных данных, а также иные руководители Учреждения, разрешающие доступ Работников к документу, содержащему защищаемую информацию, несут персональную ответственность за данное разрешение.

7.2. Защита прав субъектов персональных данных осуществляется судом, в целях пресечения неправомерного использования этих персональных данных, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.

7.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту конфиденциальной информации, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и

уголовной ответственности в порядке, установленном федеральными законами.

8. Заключительные положения

8.1. Администратор, лицо, ответственное за организацию обработки персональных данных, пользователи ИС обязаны не реже одного раза в полгода ознакомляться с настоящим документом.

8.2. Администратор, совместно с лицом, ответственным за организацию обработки персональных данных, обязаны не реже одного раза в год пересматривать и приводить в соответствие законодательству и иных нормативных актов положения настоящего документа.