Комитет образования и науки администрации города Новокузнецка
МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ
НЕТИПОВОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ГИМНАЗИЯ № 48»

Система менеджмента качества
МБ НОУ «ГИМНАЗИЯ № 48»

Согласовано:
Педагогическим советом
Протокол №01 от 31.08 2020 г.

Утверждаю
Директор МБ НОУ «Гимназия № 48»
_____ С.И. Каковихина
Приказ от «09» 09 2020 г. №200/1-ОД

Положение
об обеспечении безопасности персональных данных
при их обработке в информационных системах персональных данных
МБ НОУ «Гимназия № 48»

1. Общие положения.

1.1. Настоящее Положение устанавливает требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных МБ НОУ «Гимназия № 48» (далее - Гимназия).

1.2. Настоящее Положение разработано на основе Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных в Гимназии, определяются с учетом:

- нормативно-методических документов Гимназии;
- модели угроз и нарушителей информационной безопасности Гимназии;
- нормативных документов Гимназии в области обеспечения информационной безопасности.
- основных направлений принципов информационной безопасности Гимназии.
- актуальными для Гимназии угрозами информационной безопасности, определенными в модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных Гимназии.

1.3. В Положении используются следующие основные термины и определения:

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- информационная система персональных данных - 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;
- оператор – Гимназия, осуществляющая обработку персональных данных, а также определяющая цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- информационная безопасность - состояние защищенности интересов (целей) Гимназии в условиях угроз в информационной сфере.

Защищенность достигается обеспечением совокупности свойств информационной безопасности - доступности, целостности, конфиденциальности информационных активов. Приоритетность свойств информационной безопасности определяется ценностью указанных активов для интересов (целей) Гимназии.

- блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения 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»;

1.4. К информационным системам персональных данных Гимназии (далее – ИСПДн) относятся системы, целью создания и использования которых является обработка персональных данных (Приложение №1).

1.5. Гимназия не осуществляет трансграничную передачу персональных данных. Все технические средства ИСПДн Гимназии находятся в пределах Российской Федерации.

1.6. Согласно Указанию от 10.12.2015 г. № 3889-У "Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных, в информационных системах персональных данных" выделена Типовая модель угроз безопасности персональных данных, актуальная при их обработке в информационных системах персональных данных (Приложение №2).

В соответствии со спецификой ИСПДн Гимназии, угрозы утечки персональных данных по техническим каналам являются для Гимназии не актуальными.

1.7. Гимназия с целью выполнения обязанностей работодателя в связи с возникновением трудовых отношений между Гимназией и ее работником, а так же по оказанию образовательных услуг в пределах устава Гимназии осуществляет обработку персональных данных работников, учащихся и родителей: фамилия, имя, отчество, число, месяц и год рождения, место рождения, адресные данные, образование, профессия, семейное положение, социальное положение, паспортные данные, данные свидетельства о рождении, данные страховых свидетельств (пенсионное и медицинское), ИНН, принадлежащих работникам, состоящим в трудовых отношениях с Гимназией.

1.8. Обработка персональных данных осуществляется в режиме смешанной обработки персональных данных.

1.9. Срок или условие прекращения обработки персональных данных: ликвидация либо реорганизация Гимназии.

В случае выявления неправомерной обработки персональных данных, осуществляемой Гимназией, Гимназия в срок, не превышающий трех рабочих дней с даты этого выявления, обязана прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, Гимназия в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязана уничтожить такие персональные данные.

2. Требования по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, доступ к которым должен быть ограничен.

2.1. Требования по обеспечению безопасности персональных данных, реализуются комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации. Реализация и выполнение требований по обеспечению безопасности персональных данных должны осуществляться по согласованию и под контролем Гимназии в рамках ее полномочий.

2.2. Все информационно-вычислительные ресурсы ИСПДн Гимназии защищаются от воздействий вредоносного кода.

2.3. Обязанности по администрированию средств защиты и механизмов защиты, реализующих требования по обеспечению антивирусной защиты возлагаются приказами (распоряжениями) директора Гимназии.

2.4. Технические средства, их составные части, включая корпус, блоки, задействованные в обработке персональных данных, и отдельные, не используемые в технологическом процессе элементы указанных технических средств (например, порты, дисководы, разъемы), должны использоваться с контролем доступа, позволяющим осуществлять полноценный контроль доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации.

2.5. Сотрудники, осуществляющие обработку персональных данных в ИСПДн Гимназии, должны соблюдать требования нормативных и иных актов (регламенты, инструкции) в области информационной безопасности.

2.6. К ИСПДн требования по защите информации от утечки по техническим каналам, в том числе, по каналам побочных электромагнитных излучений и наводок не предъявляются, в соответствии с Типовой моделью угроз (Приложение №2).

2.7. Процессы обработки персональных данных, а также порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств регламентируются директором Гимназии.

2.8. Эталонные копии ПО учитываются, доступ к ним ограничен.

2.9. Восстановление ИСПДн Гимназии в случае нештатной ситуации должно осуществляться администрацией Гимназии.

2.11. Пользователям ИСПДн Гимназии запрещается осуществление несанкционированного копирования персональных данных. С этой целью в помещениях, в которых размещаются технические средства обработки персональных данных, запрещается осуществление несанкционированного копирования, в том числе, с использованием отчуждаемых носителей информации, мобильных устройств копирования и переноса информации, коммуникационных портов и устройств ввода-вывода, реализующие различные интерфейсы (включая беспроводные), запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов и т.д.), а также устройств фото- и видеосъемки.

2.12. Передача персональных данных производится государственным органам или по официальному запросу в рамках законодательства. Между Гимназией, с одной стороны, и внешними организациями, с другой стороны, передача осуществляется с использованием сертифицированных средств криптографической защиты или иных защитных механизмов.

2.13. Сохранность и целостность программных средств обеспечения информационной безопасности, персональных данных, а также других программных средств ИСПДн Гимназии является обязательной и обеспечивается, в том числе, за счет создания резервных копий.

3. Контроль обеспечения безопасности персональных данных при их обработке в ИСПДн

3.1. Контроль обеспечения безопасности персональных данных при их обработке в ИСПДн Гимназии (далее – Контроль) является неотъемлемой частью общего комплекса мер обеспечения безопасности и защиты информации Гимназии.

3.2. Контроль должен осуществляться на всех этапах обработки персональных данных.

3.3. Выделяется внутренний и внешний контроль.

3.3.1. Внешний контроль осуществляется в рамках следующих контрольных мероприятий:

- контроль и надзор за выполнением требований по обеспечению безопасности персональных данных при их обработке ИСПДн, осуществляемый ФСТЭК России и ФСБ России в пределах их полномочий;

3.3.2. Внутренний контроль осуществляется в рамках следующих контрольных мероприятий:

- мониторинг и контроль защитных мер;

- внутренние проверки (и самооценки) соответствия требованиям настоящего документа безопасности и защиты информации Гимназии;

3.4. Методическое руководство и контроль выполнения требований настоящего Порядка осуществляется Гимназией.

4. Порядок хранения материальных носителей ПД от несанкционированного доступа:

4.1. К носителям ПД в Гимназии относятся:

- бумажные (любой документ, содержащий в себе ПД сотрудника, учащегося, родителей или законных представителей) .
- электронные внутренние / стационарные, (HDD-диски ПК)
- электронные внешние / съёмные (CD, Flash-накопители и т.д.)

4.2. Хранение информации на бумажных или на электронных носителях происходит в сейфах и архиве Гимназии;

4.3. Хранение отчуждаемых (съемных) носителей ИСПДн допускается в одном хранилище с другими документами, в отдельном контейнере, опечатываемом директором Гимназии, исключающем их непреднамеренное уничтожение.

4.5. Ограничен круг лиц, имеющих парольный доступ к электронным базам данных, содержащих персональные данные. (Приложение №3)

5. Обязанности Гимназии по уточнению, блокированию и уничтожению персональных данных.

5.1. В случае выявления неправомерной обработки или при выявлении неточностей в обрабатываемых персональных данных субъектом персональных данных или его представителем необходимо, чтобы было составлено по данному случаю заявление. Гимназия обязана осуществить уточнение обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование в случае неправомерной обработки (в том числе, если обработка персональных данных осуществляется другим лицом, действующим по поручению Гимназии) с момента получения данного заявления на время проверки полученной информации.

5.2.В случае подтверждения факта неточности персональных данных Гимназия на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязана уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Гимназии) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

5.3.В случае выявления неправомерной обработки персональных данных, осуществляемой Гимназией или лицом, действующим по поручению Гимназии, Гимназия в срок, не превышающий трех рабочих дней с даты этого выявления, обязана прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Гимназии. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Гимназия обязана уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

5.4. В случае достижения цели обработки персональных данных Гимназия обязана прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению

Гимназии) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Гимназии) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено:

- договором, стороной которого является субъект персональных данных;
- соглашением между Гимназией и субъектом персональных данных.

5.5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Гимназия обязана прекратить их обработку, а также в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

6. Способы уничтожения персональных данных

1. Физическое уничтожение носителя
2. Уничтожение информации с носителя

Бумажный носитель. Уничтожение происходит через шредирование (измельчение) или уничтожение через термическую обработку (сжигание).

Электронный носитель. Уничтожение заключается в удалении информации с носителя путём многократной перезаписи в секторах магнитного диска или уничтожение самого носителя путём нанесения ему неустранимых физических повреждений, исключающих возможность его использования или восстановления ключевой информации.

Уничтожение персональных данных проводится комиссией в количестве не менее трех человек. После уничтожения составляется акт (Приложение № 4).

Приложение №1
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных.
МБ НОУ «Гимназия № 48»

Перечень информационных систем,
в которых обрабатываются персональные данные
МБ НОУ «Гимназия № 48»

№ п/п	Наименование системы	Сотрудники, допущенные директором Гимназии к работе с системой
1.	https://bus.gov.ru Официальный сайт для размещения информации о государственных (муниципальных) учреждениях	Зам. директора по ИКТ.
2.	http://zakupki.gov.ru Портал Закупок	Зам. директора по ИКТ
3.	http://dper.gisee.ru Модуль «Информация об энергосбережении и повышении энергетической эффективности»	Зам. директора по ИКТ Зам. директора по ХР
4.	http://obr.doxcell.ru Сервер «Образование»	Зам. директора по ИКТ Зам. директора по ХР Зам. директора по УВР
5.	http://mon.kuz-edu.ru Автоматизированная информационная система «Образование Кемеровской области»	Зам. директора по ИКТ, Специалист отдела кадров, Заместители директора
6.	https://vpr.statgrad.org Всероссийские проверочные работы Информационный портал	Зам. директора по ИКТ Зам. директора по УВР
7.	http://sdo.rusal.ru Корпоративный Университет РУСАЛ Система Дистанционного Обучения	Зам. директора по ИКТ, педагоги Гимназии
8.	https://ruobr.ru «Электронная школа 2.0»	Зам. директора по ИКТ, педагоги Гимназии
9.	https://gymn48.ucoz.ru Официальный сайт Гимназии	Зам. директора по ИКТ
10.	Gymnasium48@mail.ru Электронная почта Гимназии	Секретарь, Заместители директора

Приложение №2
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных
МБ НОУ «Гимназия № 48»

**Типовая модель угроз безопасности персональных данных,
актуальная при их обработке в информационных системах персональных данных
МБ НОУ «Гимназия № 48»:**

1. угроза несанкционированного доступа к персональным данным лицами, обладающими полномочиями в информационной системе персональных данных, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационной системы персональных данных;

2. угроза воздействия вредоносного кода, внешнего по отношению к информационной системе персональных данных;

3. угроза использования методов социального инжиниринга к лицам, обладающим полномочиями в информационной системе персональных данных;

4. угроза несанкционированного доступа к отчуждаемым носителям персональных данных;

5. угроза утраты (потери) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных;

6. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в организации защиты персональных данных;

7. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в программном обеспечении информационной системы персональных данных;

8. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;

9. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационной системы персональных данных;

10. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации.

Приложение №3
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных
МБ НОУ «Гимназия № 48».

Требования к организации парольной защиты
МБ НОУ «Гимназия № 48»

1. Пароли формируются заместителем директора по ИКТ Гимназии.
2. Не допускается использование единого пароля для доступа к различным информационным ресурсам Гимназии.
3. К структуре паролей предъявляются следующие требования:
   - пароль должен состоять не менее чем из 6 символов;
   - в числе символов пароля обязательно должны присутствовать буквы и цифры;
   - пароль не должен включать легко вычисляемые сочетания символов (например, имена, фамилии, наименования АРМ), какую- либо личную информацию о пользователе, а также общепринятые сокращения (например, ЭВМ, ЛВС, SYSOP);
4. при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 4 символа.
5. Свой пароль пользователь не имеет права сообщать никому. Запрещается оставлять пароли в легкодоступном или на видном месте.
6. Полная плановая смена паролей должна проводиться не реже одного раза в год.
7. Внеплановые удаление или смена пароля пользователя ИСПДн Гимназии в случае прекращения или любого изменения его полномочий должны производиться немедленно после окончания последнего сеанса работы данного пользователя. При этом должна быть также выполнена безотлагательная корректировка прав доступа на всех средствах вычислительной техники в соответствии с изменившимися полномочиями сотрудника.
8. Внеплановая полная смена паролей должна производиться в случае прекращения полномочий администраторов (увольнение, переход на другую работу внутри Гимназии и другие обстоятельства) и других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению автоматизированной системой в целом, либо полномочия по управлению подсистемой защиты информации данной автоматизированной системы, а значит, кроме личного пароля им могут быть известны пароли других пользователей системы.
9. В случае компрометации пароля (подсматривание его кем-либо, разглашение пароля и др.) пароль необходимо сменить.

Приложение №4
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных
МБ НОУ «Гимназия № 48»

РАЗРЕШАЮ УНИЧТОЖИТЬ
Директор
МБ НОУ «Гимназия № 48»
_____Каковихина С.И.

“		”		20__г

Акт об уничтожении персональных данных

Комиссия, назначенная приказом по Гимназии № ___ от _____ ___ г. для уничтожения персональных данных, в составе:
Председатель комиссии: _____ ;
Члены комиссии: _____ ;
_____ .
провела отбор носителей персональных данных _____ для уничтожения по реестру от «__» _____ ___ г. и установила, что персональные данные, полученные в результате обработки

_____,
(наименование отделов)
в соответствии с требованиями руководящих документов по защите информации, подлежат уничтожению, в связи с

_____ .
(цель обработки данных достигнута, утрата необходимости в достижении целей обработки и т.д.)

№ п/п	Дата	Тип носителя	Кол-во листов

Всего подлежит уничтожению: _____ (_____) носителей.
цифрами прописью

Комиссия установила, что после утверждения Акта об уничтожении персональных данных перечисленные носители сверены с записями в Акте и уничтожены путем

_____
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Председатель комиссии:		/	
Члены комиссии:		/	
		/	