УТВЕРЖДАЮ
Директор ГОУ ЯО
«Рыбинская школа-интернат № 2»
_____О.Н. Руденко

Приказ № 47 от «31» августа 2018 г.

СОГЛАСОВАНО
на заседании Совета учреждения
Протокол № 1 от «30» августа 2018 г.

Правила

доступа к персональным данным, обрабатываемым в информационной системе персональных данных

государственного общеобразовательного учреждения
Ярославской области
«Рыбинская школа-интернат № 2

I. Общие положения

1.1. Правила обработки персональных данных в государственном общеобразовательном учреждении Ярославской области «Рыбинская школа – интернат № 2» (далее- Правила) определяют цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также мероприятия , направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных ГОУ ЯО «Рыбинская школа – интернат № 2» (далее – Учреждение).
1.2. Настоящие Правила определяют политику Учреждения как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.
1.3. В целях настоящих Правил используются следующие понятия:
-**автоматизированная** обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;
- **блокирование** персональных данных – временное прекращение обработки
персональных данных (за исключением случаев, если обработка необходима дляуточнения персональных данных);
-информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
-конфиденциальность персональных данных – обязанность оператора и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;
-обезличивание персональных данных - действия, в результате которых становиться невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
-**обработка персональныхданных** - 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 – работник Учреждения, самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными при предоставлении государственных услуг;

-персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
-предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
-распространение персональных данных- действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
-трансграничная передачаперсональных данных - передача персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
-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. Настоящие Правила разработаны в соответствии с

- Трудовым кодексом Российской Федерации,
- Кодексом Российской Федерации об административных правонарушениях, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»,
- Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 6 июля 2008 г. N 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»,
- постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,
- постановлением Правительства Российской Федерации от 21 марта 2012 г. N 211 «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»,
- приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»; Федеральным законом Российской Федерации от 29 декабря 2012 г. № 273 – ФЗ «Об образовании в Российской Федерации».

1.5.Обработка персональных данных в Учреждении осуществляется с соблюдением порядка и условий, предусмотренных настоящими Правилами и законодательством Российской Федерации в области персональных данных.

1.6. В Учреждении ведется обработка персональных данных следующих категорий субъектов персональных данных:
- учащихся их родителей (законных представителей);
- работников школы – интерната.

II. Условия и порядок обработки персональных данных работников Учреждения

2.1. Персональные данные учащихся, их родителей (законных представителей) Учреждения обрабатываются в связи с образовательной деятельностью. Персональные данные работников Учреждения обрабатываются в целях обеспечения кадровой и бухгалтерской работы, а также в целях обучения и должностного роста, учета результатов исполнения работниками должностных обязанностей, обеспечения им условий труда, гарантий и компенсаций.
2.2. В целях, указанных в пункте 2.1. настоящих Правил, обрабатываются следующие категории персональных работников;

- фамилия, имя, отчество учащегося, его родителей (законных представителей), сотрудника;
- дата рождения учащегося, его родителей (законных представителей), сотрудника;
- паспортные данные родителей (законных представителей), сотрудников;
- данные свидетельства о рождении учащихся;

- сведения о месте работы (учебы) родителей (законных представителей);
- адрес регистрации и проживания, контактные телефоны, адрес электронной почты;
- иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 2.1. настоящих Правил.

2.2.1. Документами, содержащими персональные данные являются:

1) паспорт или иной документ, удостоверяющий личность учащегося, его родителей (законных представителей), сотрудника
2) трудовая книжка;
3) страховое свидетельство государственного пенсионного страхования;
4) свидетельство о постановке на учет в налоговый орган и присвоения ИНН;
5) документы воинского учета;
6) документы об образовании, о квалификации или наличие специальных знаний или специальной подготовки;
7) карточка Т-2;
8) автобиография;
9) личный листок по учету кадров;
10) медицинское заключение о состоянии здоровья;
11) документы, содержащие сведения о заработной плате, доплатах и надбавках;
12) приказы о приеме лица на работу, об увольнении, а также переводе лица на другую должность;
13) семейное положение, состав семьи и сведения о близких родственниках;
14) фотография;
15) номер расчетного счета.
16) иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 2.1. настоящих Правил.
2.3. Обработка персональных данных работников осуществляется в соответствии с Трудовым кодексом Российской Федерации.
2.4. Обработка персональных данных работников осуществляется при условии получения от них письменного согласия на обработку персональных данных в следующих случаях;

- при передаче (распространении, предоставлении) их персональных данных третьим лицам, кроме случаев, предусмотренных действующим законодательством Российской Федерации;
- при принятии решений, порождающих юридические последствия в отношении работников или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных;

2.5. В случаях, предусмотренных пунктом 2.4. настоящих Правил, согласие работника на обработку его персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных». Форма согласия утверждается приказом директора.
2.6. Непосредственная обработка персональных данных учащихся, их родителей (законных представителей) и сотрудников Учреждения осуществляется инспектором по кадрам, специалистов бухгалтерии, зам. директоров по УР, ВР, АХЧ и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.7. Специалисты, работающие в информационных системах обеспечивают хранение информационных баз с персональными данными работников.
2.8. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных работников, а также граждан, претендующих на замещение вакантных должностей, осуществляется путем:

- получения оригиналов необходимых документов (заявления, трудовая книжка иные документы, предоставляемые в отдел кадров и бухгалтерии);
- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- формирования персональных данных в ходе кадровой работы;
- внесения персональных данных в информационные системы персональных данных, используемые инспектором по кадрам, специалистами бухгалтерии, зам. директором по ВР, УР, АХР.

2.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных работников осуществляется путем получения персональных данных непосредственно от работников, а также граждан, претендующих на замещение вакантных должностей.
2.10. В случае возникновения необходимости получения персональных данных работника, у третьей стороны, следует известить об этом работника заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных.
2.11. Запрещается получать, обрабатывать и приобщать к личному делу работника персональные данные, не предусмотренные пунктом 2.2. настоящих Правил, в том числе касающейся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.
2.12. При сборе персональных данных инспектор по кадрам осуществляющий сбор (получение) персональных данных непосредственно от работников, а также граждан, претендующих на замещение вакантных должностей, обязан разъяснить указанным субъектам персональных данных юридических последствий отказа представить свои персональные данные в связи с поступлением на работу и её выполнением в Учреждении.
2.13. Передача (распространение, предоставление) и использование персональных данных работников, а также граждан, претендующих на замещение вакантных должностей, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

III. Порядок обработки персональных данных субъектов персональных данных в информационных системах персональных данных в Учреждении

3.1. Обработка персональных данных субъектов персональных данных осуществляется в:
- автоматизированной системе информационного обеспечения управления АСИОУ – учебная часть, кадры;
- автоматизированной системе «1 С Предприятие», «Клиент- Сбербанк», «Сбис ++ электронная отчетность» - бухгалтерия;
- автоматизированной системе «Перечень ЛП» - кадры.

3.2. Информационные системы содержат персональные данные учащихся их родителей (законных представителей) и сотрудников Учреждения, предусмотренные пунктом 2.2. настоящих Правил и обеспечивают работу образовательной, финансовой и трудовой деятельности.
3.3. Автоматизированные рабочие места сотрудников Учреждения, предполагают обработку персональных данных согласно пункту 2.2. настоящих Правил.

3.4. Классификация информационных систем персональных данных Учрежденияосуществляется в порядке, установленном законодательством Российской Федерации.
3.5. Сотрудникам Учреждения, имеющим право осуществлять обработку персональных данных в информационных системах персональных данных, подписывается Обязательство. В случае расторжения с ним трудового договора, о неразглашении. Таким работникам предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе персональных данных. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными обязанностями работников.
Информация с персональными данными вносится в базы с персональными данными и в другие места хранения информации в электронном виде в ручном режиме, при получении информации на бумажном носителе.
3.6. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:
а) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
б) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
в) применение прошедших в установленном порядке процедур оценки соответствия, средств защиты информации;
г) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
д) учет машинных носителей персональных данных;
е) обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
ж) восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;
з) установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;
и) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.
3.7. Системный администратор несет ответственность за обеспечение информационной безопасности в Учреждении, в том числе разрабатывает и организует меры по обеспечению безопасности персональных данных, а также организует и контролирует ведение учета материальных носителей персональных данных.
3.8. Системный администратор обеспечивает:
1) своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до директора и ответственного за организацию безопасной обработки персональных данных Учреждения;
2) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
3) возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
4) постоянный контроль за обеспечением уровня защищенности персональных данных;

5) соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
6) учет носителей персональных данных и применяемых средств защиты информации, эксплуатационной и технической документации к ним;
7) при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных вплоть до выявления причин нарушений и устранения этих причин;
8) разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.
3.9. Системный администратор, принимает все необходимые меры по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.
3.10. Обмен персональными данными при их обработке в информационных системах персональных данных осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.
3.11. Доступ работников к персональным данным, размещенным в информационных системах персональных данных, предусматривает обязательное прохождение процедуры идентификации и аутентификации.
3.12. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

IV. Сроки обработки и хранения персональных данных

4.1. Сроки обработки и хранения документов с персональными данными работников, а также граждан, претендующих на замещение вакантных должностей, определяются в соответствии с законодательством Российской Федерации. С учетом положений законодательства Российской Федерации, устанавливаются следующие сроки обработки и хранения персональных данных работников:
1) персональные данные, содержащиеся в приказах по личному составу
(о приеме, о переводе, об увольнении, об установлении надбавок о поощрениях, о материальной помощи и т.д.), подлежат хранению в службе кадров в течение 75 лет;
2) документы, содержащие персональные данные работников, в том числе сведения о заработной плате, подлежат хранению в бухгалтерии в течение 75 лет.
4.2. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).
4.3. В Учреждении обеспечивается раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящими Правилами.
4.4. Контроль за хранением и использованием материальных носителей персональных данных, не допускающих несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют руководители структурных подразделений, осуществляющих обработку персональных данных субъектов персональных данных, указанных в пункте 1.6 настоящих Правил.

4.5. Срок хранения персональных данных, внесенных в информационные системы персональных данных Учреждения не должен превышать установленный в согласии на обработку персональных данных срок.

V. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

5.1. Учреждение осуществляет систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения и подлежащих уничтожению.

5.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании комиссии, состав которой утверждается приказом директора.

По итогам заседания составляются протокол и акт о выделении к уничтожению документов, опись уничтожаемых дел; дела проверяются на их комплектность, акт подписывается председателем и членами комиссии и утверждается директором.

5.3.Уничтожение документов, содержащих персональные данные, производится членами комиссии путем сжигания или аппаратного измельчения.

5.4. По окончании процедуры уничтожения, комиссией составляется соответствующий акт об уничтожении документов, содержащих персональные данные.

5.5. Уничтожение персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или программным удалением необходимой информации принятыми для конкретного типа носителя методами.

VI. Ответственные за организацию обработки персональных данных В Учреждении

6.1. Директором Учреждения из числа заместителей назначается ответственный за организацию режима защиты информации, в том числе за организацию безопасной обработки персональных данных, который курирует вопросы защиты информации в ГОУ ЯО «Рыбинская школа – интернат № 2». В полномочия заместителя, ответственного за организацию безопасной обработки персональных данных, входит:

1) принятие правовых, организационных и технических мер для обеспечения защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

2) организация внутренних проверок на предмет соблюдения работниками требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

3) инициирование разработки локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

4) организация контроля приема и обработки обращений и запросов от субъектов персональных данных;

5) в случае нарушения в Учреждении требований к защите персональных данных, принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

6.2. Заместитель, ответственный за организацию безопасной обработки персональных данных, вправе привлекать к реализации вышеуказанных мер по защите информации иных работников Учреждения с возложением на них соответствующих обязанностей и

закреплением ответственности, а также вправе иметь доступ к информации, касающейся обработки персональных данных и включающей:

- цели обработки персональных данных;
- категории обрабатываемых персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовые основания обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых в Учреждении способов обработки персональных данных;
- описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- дату начала обработки персональных данных;
- срок или условия прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

6.3. Непосредственное руководство работами, направленными на обеспечение защиты персональных данных, а также контроль проводимых работ обеспечивает специалист (по безопасности) отдела информационных систем, которому могут быть делегированы (переданы) полномочия, перечисленные в пункте 6.2.

Специалист (по безопасности) отдела информационных систем участвует в разработке внутренних нормативных документов по защите персональных данных.

6.4. Сотрудники службы кадров и бухгалтерии, а также заместители директора по УР, ВР и АХР несут персональную ответственность за соблюдение установленного режима обработки персональных данных субъектов персональных данных, указанных в пункте 1.6 настоящих Правил.

6.5. Должностные лица, указанные в пунктах 6.1 - 6.4 настоящих Правил, при проведении работ, связанных с обработкой персональных данных, руководствуются законодательством Российской Федерации в области персональных данных и настоящими Правилами.

6.6. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, установленных Федеральным законом «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.