Министерство образования Белгородской области
Областное государственное автономное
профессиональное образовательное учреждение
«ЯКОВЛЕВСКИЙ ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ»

ПРИНЯТО
на заседании Общего собрания
ОГАПОУ ЯПК
Протокол №_1_ от «31» 08 2026 г.

УТВЕРЖДАЮ
Директор ОГАПОУ ЯПК
Подписано цифровой подписью: Шепелева Жанна Николаевна
DN: cn=Шепелева Жанна Николаевна, o=ОГАПОУ ЯПК, ou, email=jakpu@belregion.ru, c=RU
Дата: 2026.11.03 15:26:38 +03'00'
_____Ж.Н. Шепелева
Приказ № 601-ОС от «_1_»_09___2026 г.

Положение об обеспечении безопасности персональных данных Областного государственного автономного профессионального образовательного учреждения «Яковлевский педагогический колледж»

Строитель 2026

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (с учетом изменений, внесенных Федеральными законами от 24.06.2025 № 156-ФЗ и от 30.11.2024 № 420-ФЗ), Постановлением Правительства РФ от 01.11.2012 № 1119, Приказом ФСТЭК России от 18.02.2013 № 21.

1.2. Положение определяет политику ОГАПОУ «Яковлевский педагогический колледж» (далее — Оператор/Колледж) в отношении обработки и защиты персональных данных (ПДн), а также процедуры, направленные на предотвращение и выявление нарушений законодательства РФ.

1.3. Основные термины используются в значениях, установленных ст. 3 ФЗ-152. Вводятся дополнительные понятия:

- **Локализация:** требование по первичному сбору и хранению ПДн граждан РФ в базах данных на территории РФ.
- **Обезличивание:** действия, в результате которых без использования дополнительной информации невозможно определить принадлежность ПДн конкретному субъекту.

2. Цели и правовые основания обработки

2.1. Цели обработки: обеспечение образовательного процесса, соблюдение трудового законодательства, ведение бухгалтерского учета, исполнение государственных контрактов, организация пропускного режима.

2.2. Правовые основания: ФЗ-152, ФЗ «Об образовании в РФ», Трудовой кодекс РФ, Устав Колледжа, договоры с субъектами ПДн.

3. Порядок и условия обработки персональных данных

3.1. Обработка ПДн осуществляется с согласия субъекта, за исключением случаев, предусмотренных ст. 6 ФЗ-152 (исполнение договора, выполнение обязанностей по закону).

3.2. **Требование к форме согласия (с 01.09.2025):** Согласие на обработку ПДн оформляется исключительно как отдельный документ. Запрещается включать текст согласия в состав трудовых договоров, договоров об оказании платных образовательных услуг, пользовательских соглашений на сайте, анкет или оферт. Каждое согласие должно содержать: ФИО и паспортные данные субъекта, реквизиты Оператора, конкретные цели обработки, перечень ПДн, перечень действий с данными, срок действия и способ отзыва.11 источников

3.3. **Требование к локализации (с 01.07.2025):** Первичный сбор, запись, систематизация и накопление ПДн граждан РФ осуществляются с использованием баз данных, находящихся на территории Российской Федерации. Использование зарубежных облачных сервисов для первичного сбора данных (анкет абитуриентов, заявок) запрещено.

3.4. **Передача обезличенных данных (с 01.09.2025):** По запросу Минцифры России Оператор обязан передавать обезличенные ПДн в государственную информационную систему (ГИС). Биометрические и специальные категории ПДн в ГИС не передаются. Методы обезличивания утверждаются Правительством РФ.2 источника

3.5. Хранение ПДн осуществляется не дольше, чем этого требуют цели обработки. По достижении целей ПДн подлежат уничтожению или обезличиванию в срок, не превышающий 30 дней.

4. Организация работ по обеспечению безопасности

4.1. Ответственным за организацию обработки ПДн является заместитель директора по административно-хозяйственной работе.

4.2. Ответственным за обеспечение безопасности ПДн в ИСПДн (Администратором безопасности) является начальник отдела информационных технологий.

4.3. Для защиты ПДн Оператор реализует следующие меры:

- Назначение ответственных лиц (п. 4.1, 4.2).
- Ограничение доступа: доступ к ПДн предоставляется только тем работникам, которым он необходим для выполнения должностных обязанностей (на основании приказов и должностных инструкций).
- Разработка и утверждение локальных актов: настоящего Положения, Перечня ИСПДн, Перечня должностей, имеющих доступ к ПДн, Регламента резервного копирования, Регламента уничтожения носителей.
- Применение сертифицированных средств защиты информации (антивирусное ПО, межсетевые экраны, средства защиты от несанкционированного доступа).
- Учет и хранение материальных носителей ПДн (личные дела, журналы, зачетные книжки) в сейфах или запираемых шкафах.
- Контроль за локализацией: ежеквартальная проверка фактического расположения серверов и облачных баз данных на территории РФ.

5. Проведение работ по обеспечению безопасности

5.1. Внутренний контроль соответствия обработки ПДн законодательству проводится не реже одного раза в полугодие.

5.2. При приеме на работу каждый сотрудник обязан ознакомиться под подпись с настоящим Положением и подписать отдельное Обязательство о неразглашении ПДн.

5.3. В ИСПДн ведется автоматизированный лог-файл действий пользователей.

5.4. Резервное копирование баз данных производится не реже одного раза в сутки. Резервные копии хранятся на территории РФ.

5.5. **Уведомление Роскомнадзора:** Колледж обязан уведомить Роскомнадзор о начале обработки ПДн (если отсутствуют основания для исключения по ч. 2 ст. 22 ФЗ-152).

5.6. **Инциденты (с 30.05.2025):** В случае утечки данных Оператор обязан уведомить Роскомнадзор в течение 24 часов с момента обнаружения инцидента и в течение 72 часов предоставить результаты внутреннего расследования.

5.7. При выявлении неточностей в ПДн по обращению субъекта, Оператор обязан внести уточнения в течение 7 рабочих дней.

6. Ответственность

6.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут дисциплинарную, административную (ст. 13.11 КоАП РФ), гражданско-правовую и уголовную (ст. 137 УК РФ) ответственность в соответствии с федеральным законодательством.

6.2. Оператор несет ответственность за нарушение требований по локализации баз данных в виде административного штрафа.