**Памятка руководителю о требованиях к информационной безопасности в ОО.**

1. Обработка персональных данных работников допускается в случаях, если субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
2. Обработка персональных данных детей допускается в случаях, если согласие на обработку его персональных данных дали родители или законные представители в письменной форме;
3. Каждая школа разрабатывает локальный акт, который конкретизирует сведения, относящиеся к персональным данным, кто имеет доступ к персональным данным обучающегося, права и обязанности работников, получивших доступ к персональным данным ученика и т. д.;
4. Не существует единой формы согласия на обработку персональных данных, эту форму разрабатывает школа, необходимо только, чтобы она содержала все необходимые сведения согласно требованиям ч. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
5. Размещение фото и видеоизображений на официальных сайтах образовательных учреждений без письменного согласия законных представителей субъектов персональных данных запрещено;
6. В Реестре операторов персональных данных должны содержаться актуальные сведения об ОО. Оператор обязан сообщить об изменении сведений;
7. В ОО должны быть согласия субъекта персональных данных при поручении обработки персональных данных учащихся образовательных учреждений третьим лицам при ведении электронных дневников. Поручение обработки персональных данных учащихся образовательных учреждений третьим лицам должно соответствовать требованиям ч. 3 ст. 6 Закона о персональных данных;
8. ОО обязана издать документы, определяющие политику оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушении законодательства Российской Федерации, устранение последствий таких нарушений. Эти нормативные документы должны быть размещены в разделе сайта ОО «Информационная безопасность»;
9. В ОО должен быть стенд, посвященный информационной безопасности;
10. Компьютеры в ОО должны иметь систему фильтрации интернет-контента (СФК).