Утверждаю
Директор МОУ Иванковской СОШ:
_____ Г.В. Жаренова
Приказ № 175 от 01.09.2014г.

ПРАВИЛА
ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, а также локальными актами МОУ Иванковская СОШ (далее – Учреждение) (далее – Правила) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных, основания, порядок, формы и методы проведения внутреннего контроля за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

2. Настоящие Правила разработаны в соответствии с требованиями пункта 4 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3. В целях осуществления внутреннего контроля за соблюдением законодательства Российской Федерации в области персональных данных в Учреждении проводятся плановые (периодические) и внеплановые проверки.

4. Плановые (периодические) и внеплановые проверки проводятся ответственным за организацию обработки персональных данных или комиссией, назначаемой приказом руководителя Учреждения. Количественный состав участников комиссии должен быть не менее трех должностных лиц, в том числе должностное лицо, отвечающее за вопросы правового обеспечения и должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе (при наличии) Администратор безопасности информационной системы персональных данных.

5. В проведении проверки не может участвовать работник прямо или косвенно заинтересованный в ее результатах.

6. Плановые (периодические) проверки проводятся на основании ежегодного плана проведения плановых (периодических) проверок на текущий календарный год (далее – План).

7. План утверждается директором Учреждения.

8. Внеплановые проверки проводятся по следующим основаниям:

8.1. Истечение срока исполнения Учреждением ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства Российской Федерации в области персональных данных.

8.2. Поступление в Учреждение обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о следующих фактах:

8.2.1. Возникновение угрозы причинения вреда жизни, здоровью граждан.

8.2.2. Причинение вреда жизни, здоровью граждан.

8.2.3. Нарушение прав и законных интересов граждан действиями (бездействием) Учреждения или лицами, осуществляющими обработку персональных данных по поручению Учреждения при обработке их персональных данных.

8.2.4. Нарушение Учреждением или лицами, осуществляющими обработку персональных данных по поручению Учреждения требований законодательства Российской

Федерации в области персональных данных, а также о несоответствии сведений, содержащихся в уведомлении об обработке персональных данных, фактической деятельности.

8.3. На основании приказа руководителя Учреждения.

9. Обращения и заявления, не позволяющие установить лицо, обратившееся в Учреждение, а также обращения и заявления, не содержащие сведений о фактах, указанных в подпункте 8.2 пункта 8 настоящего Порядка, не могут служить основанием для проведения внеплановой проверки.

10. Срок проведения как плановой (периодической), так и внеплановой проверки не может превышать десяти рабочих дней.

11. В случае возникновения необходимости срок проведения проверки может быть продлен, но на срок не более десяти рабочих дней. При необходимости продления срока проверки, должностные лица, проводящие проверку: ответственный за организацию обработки персональных данных в Учреждении, либо члены комиссии, назначенные приказом руководителя Учреждения не позднее, чем за два дня до даты окончания проверки готовят докладную записку с изложением причин продления срока и направляют ее руководителю Учреждения.

12. Приказ о продлении проверки подготавливается в сроки, установленные в Учреждении, но не позднее двух рабочих дней, со дня принятия решения о продлении сроков проверки руководителем Учреждения.

13. При необходимости изменения состава комиссии, проводящей проверку, в Учреждении издается соответствующий приказ.

14. В ходе проведения проверки, ответственный за организацию обработки персональных данных или комиссия должны оценить соответствие деятельности Учреждения требованиям, установленным нормативными правовыми актами в области персональных данных, удостовериться в полноте и достоверности сведений, содержащихся в уведомлении об обработке персональных данных, и иных имеющихся в распоряжении Учреждения документах.

При проведении проверки должны быть полностью, объективно и всесторонне определены:

- полнота и достоверность сведений, содержащихся в уведомлении об обработке персональных данных;
- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- состояние учета машинных, материальных носителей персональных данных;
- соответствие информационных систем персональных данных, утвержденному перечню информационных систем персональных данных;
- соответствие перечня персональных данных, обрабатываемых в Учреждении в связи с реализацией трудовых отношений, а также в связи с осуществлением функций и полномочий, предусмотренных законодательством Российской Федерации и в других случаях.
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- состав технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация);
- правила генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе;

- контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

- исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации;

- осуществление мероприятий по обеспечению целостности персональных данных.

Ответственный за организацию обработки персональных данных или комиссия имеет право:

- запрашивать у работников Учреждения информацию, необходимую для реализации полномочий;

- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- направлять директору Учреждения предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить директору Учреждения предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

15. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных и членам комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

16. Проверка должна быть завершена в сроки установленные планом, либо приказом о проведении проверки.

17. По результатам проверки должностными лицами, проводившими проверку, составляется акт проверки, который оформляется непосредственно после ее завершения.

18. В акте проверки указываются:

18.1. Дата, время и место составления акта проверки.

18.2. Основания проведения проверки.

18.3. Фамилии, имена, отчества должностных лиц, проводивших проверку.

18.4. Дата, время и продолжительность проведения проверки.

18.5. Сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований законодательства Российской Федерации в области персональных данных, об их характере и о лицах, допустивших указанные нарушения.

18.6. Подписи должностных лиц, проводивших проверку.

19. Акт должен содержать одно из следующих заключений:

19.1. Об отсутствии в деятельности Учреждения нарушений требований законодательства Российской Федерации в области персональных данных.

19.2. О выявленных в деятельности Учреждения нарушениях требований законодательства Российской Федерации в области персональных данных, с указанием конкретных статей и (или) пунктов нормативных правовых актов.

20. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, ответственный за организацию обработки персональных данных или председатель комиссии докладывают директору Учреждения.

Принято на заседании педагогического
Совета МОУ Иванковской СОШ
Протокол № 1 от 29.08.2014г.