Приложение № ___ к приказу
№_____

Инструкция
по использованию персональных мобильных устройств работниками и обучающимися Центра Алмазова.

1. РАБОТНИКАМ ЗАПРЕЩАЕТСЯ:

1.1. Использовать мобильные устройства компании Apple при выполнении должностных обязанностей.
1.2. Использовать мобильные устройства во время проведения закрытых совещаний и переговоров в помещениях Центра Алмазова;
1.3. Использовать для рабочих коммуникаций (звонки; чаты; доступ к электронной почте, системам электронного документооборота и другим информационным системам):
– мессенджеры «WhatsApp» и «Viber»;
– сервисы «Google» (электронная почта, социальные сети, таблицы, карты и др.);
– «Skype»
– «Microsoft Teams».
1.4. Посредством социальных сетей вести служебную переписку, а также обрабатывать, хранить, передавать, опубликовывать и распространять служебную и иную конфиденциальную (в том числе относящуюся к охраняемой законом тайне) информацию.
1.5. Оставлять на территории Центра Алмазова видимым мобильное устройство через технологию Bluetooth, кроме моментов сопряжения с «известными» устройствами;
1.6. Использовать сервис геопозиционирования мобильного устройства (GPS) в помещениях Центра Алмазова (за исключением времени его практического использования).
1.7. Осуществлять подключение к внутренним информационным ресурсам Центра Алмазова со всех мобильных устройств компании Apple.

2. ОБУЧАЮЩИМСЯ ЗАПРЕЩАЕТСЯ:

2.1. Использовать для коммуникаций в процессе обучения (звонки; чаты; доступ к электронной почте, системам электронного документооборота и другим информационным системам):
– мессенджеры «WhatsApp» и «Viber»;
– сервисы «Google» (электронная почта, социальные сети, таблицы, карты и др.);
– «Skype»
– «Microsoft Teams».
2.2. Посредством социальных сетей вести переписку, связанную с внутренней деятельностью Центра Алмазова, а также обрабатывать, хранить, передавать, опубликовывать и распространять конфиденциальную (в том числе относящуюся к охраняемой законом тайне) информацию, а также сведения, касающиеся образовательного процесса.
2.3. Оставлять на территории Центра Алмазова видимым мобильное устройство через технологию Bluetooth, кроме моментов сопряжения с «известными» устройствами;
2.4. Использовать сервис геопозиционирования мобильного устройства(GPS) в помещениях Центра Алмазова (за исключением времени его практического использования).
2.5. Осуществлять подключение к внутренним информационным ресурсам Центра Алмазова со всех мобильных устройств компании Apple.

3. РАБОТНИКАМ И ОБУЧАЮЩИМСЯ РЕКОМЕНДОВАНО:

3.1. Использовать для рабочих и учебных целей отдельное мобильное устройство функционирующее на российской операционной системе (Аврора), либо на операционной системе «Android», с учетом отсутствия на нем установленных личных и развлекательных приложений:

- рекомендованных российских производителей: Aquarius, AYYA, F+;
- рекомендованных китайских производителей: Huawei, Xiaomi, OnePlus, Honor, Meizu и др.).

3.2. Использовать в личных целях мессенджеры: VK Мессенджер, ТамТам, eXpress, Telegram (секретные чаты), Signal;

3.3. Проверять средствами антивирусной защиты (поскольку встроенной в функционал мобильного устройства проверки пакетов недостаточно), в том числе с использованием российских антивирусных средств: Kaspersky Internet Security или Dr.Web., любых скачанных приложений, в частности, с известных «контактов» в виде файлов, интернет-ссылок, писем и сообщений.

3.4. Проводить принудительную полную антивирусную проверку мобильного устройства не реже 1 раза в месяц, а также незамедлительно при подозрении на его нештатную работу (замедление работы, подозрительная активность одного или нескольких установленных приложений).

3.5. Не использовать пин-код и графический ключ в качестве основного средства защиты от несанкционированного доступа к мобильному устройству;

3.6. Не использовать одинаковые пароли для различных ресурсов.

3.7. Использовать текстовый пароль или биометрические средства аутентификации в качестве основных средства защиты от несанкционированного доступа к мобильному устройству;

3.8. Активировать в используемых программах двухэтапную аутентификацию (SMS/push и пароль).

3.9. В целях недопущения информационных утечек и атак не публиковать и не распространять посредством социальных сетей информацию (медиаданные), касающихся личных данных, в том числе, в принадлежащих родственникам аккаунтах.

4. В СЛУЧАЕ НАХОЖДЕНИЯ НА ТЕРРИТОРИЯХ ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ, ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ, ХЕРСОНСКОЙ И ЗАПОРОЖСКОЙ ОБЛАСТЕЙ:

4.1. **ЗАПРЕЩАЕТСЯ** иметь при себе включенное мобильное устройство вблизи границы и линии боевого соприкосновения;

4.2. **НЕОБХОДИМО УСТАНОВИТЬ** в настройках телефона, касающихся определения оператора связи вручную выбор оператора связи, чья SIM-карта была приобретена, поскольку базовые станции других государств могут распространять сигнал на расстояния более 30 км.

4.3. **НЕОБХОДИМО ОТКЛЮЧИТЬ** в телефоне GPS-соединение со спутником, а в случае необходимости геопозиционирования использовать только систему ГЛОНАСС.