

## **RE32RC20: Technology and Real Estate Brokerage**

*Updated July 2020*

1. Real estate uses of technology
  - a. Marketing/Advertising
  - b. Transaction Management
  - c. Lead generation
  - d. Contact management (CRM)
  
2. Compliance
  - a. Disclosures
  - b. Broker Policies
    - i. Email
    - ii. Social media
    - iii. Websites
    - iv. Blogging
    - v. Videos
      - you tube
      - video emails
      - streaming
  - c. Email - CAN-SPAM Act
    - i. Applies to Commercial e-mail
    - ii. "Unsubscribe" must be present
    - iii. Sending duplicate emails must be avoided
    - iv. Physical location (street address) must be included in signature files for emails
  - d. Use of images/photography
    - i. Ownership of images
    - ii. Copyright issues
    - iii. Stock photography - the purchase of photos through a license for use
    - iv. Professional photography, including ownership of images
  - e. Drones (UAS)
    - i. In 2016, the FAA eliminated roadblocks for drone use for real estate agents
    - ii. Agents are free to use drones to capture aerial photos/videos to showcase homes
    - iii. Unmanned aircraft systems (UAS) must weigh less than 55 pounds and must be registered with the FAA
    - iv. Registration is valid for 3 years
    - v. Operators may only fly UAS during the daytime, under 400 feet and at less than 100 MPH
    - vi. The drone must always be in sight and yield to manned aircraft
    - vii. Drones cannot be operated from moving vehicles

3. Safeguarding Consumer Data Privacy policy
  - a. Websites/ emails
    - i. Usage policy for website visitors' personal information
    - ii. Visitor authorization of information
    - iii. Third party use of data
    - iv. Subscriptions/sign ups - how is data collected and used
    - v. Are you using a secure email ? Personal email such as comcast, verizon, yahoo, gmail, hotmail etc may not be secure.
    - vi. Best practice is to use your brokerage email for business
  - b. Written Information Security Plan (WISP)
    - i. MA Law since January 1, 2010
    - ii. For businesses that handle personal information
      1. First and last name or first initial and last name AND
      2. Social Security Number, Driver License number or financial account number
    - iii. Business is required to assess how it will safeguard personal information
  - c. General Data Protection Regulation (GDPR)
    - i. Governs how websites and business will treat data that belongs to residents of the European Union (EU)
    - ii. Applies to all businesses and organizations around the world, not just members of the EU
    - iii. Requires affirmative "opt in" to allow companies to collect website user's personal data
    - iv. The goal is to give back control of personal data to individuals
  - d. Wire Fraud
    - i. Obligation to inform clients
    - ii. Never respond to email requests,
    - iii. Notify the FBI
4. Social media/video
  - a. Salespersons Prohibited From Advertising - Salespeople are prohibited from advertising the purchase, sale, rental or exchange of any real property under their own name
  - b. Brokers should have written policies with respect to social media/video use by Salespersons
  - c. Social media accounts/postings and videos must comply with all disclosure requirements
  - d. Salespersons/Brokers using social media accounts for business purposes shall create business profiles for each account
  - e. see 254 CMR: BOARD OF REGISTRATION OF REAL ESTATE BROKERS AND SALESMEN, (9) Advertising.  
<https://www.mass.gov/doc/254-cmr-3-professional-standards-of-practice/download>

5. Dark side of Technology
  - a. The real estate industry is targeted by criminals
  - b. Tactics and focus change and evolve over time
  - c. Methods of Cyber Attacks
    - i. Social Engineering - developing new methods to manipulate users into believing a message, link or attachment is from a trusted source, then systems are attacked (Phishing, spear phishing, whaling )
    - ii. Hacking - exploiting vulnerabilities in software and hardware
    - iii. Malware - ransomware, adware, spyware, trojans, worms, viruses
    - iv. Password attack - an attack that takes advantage of the fact people tend to use common words and short passwords
    - v. Man-in-the-middle attack - an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other
    - vi. Unsecured public Wi-Fi use
    - vii. Denial-of-service - attackers send overwhelming quantities of data to a website, rendering it unusable
6. Managing risks
  - a. Password management
  - b. Computer system/device security
  - c. Records retention program
  - d. Third party vendor plans
  - e. WISP Plan  
see 201 CMR 17.00 COMPLIANCE CHECKLIST for information on The Comprehensive Written Information Security Program (WISP)  
<https://www.mass.gov/files/documents/2017/11/21/compliance-checklist.pdf>
7. Emerging Technologies
  - a. Blockchain
  - b. Virtual Reality (VR)
  - c. Augmented Reality (AR)
  - d. Automation/Machine Learning
  - e. Smartphone Apps/Push Technology
  - f. Big Data
  - g. iBuying

*\* Please note that this outline was left intentionally with slightly less detail to allow instructors the ability to teach correct and pertinent information as technology evolves and changes.*

#### **Reference Material**

- Wire Fraud FBI?
- 201 CMR 17.00 WISP