RMCC - OCR Network Improvement

Prepared by: Adam Woodall

Overview: Following a consultation with Jellyfish IT and an on-site evaluation of our building, several concerns have been identified regarding our current Wi-Fi network setup. The primary issues are security risks and inadequate Wi-Fi coverage.

Key Concerns:

1. **Single Network for Public and Office Use:**
   - Our current setup has one network shared by public and office PCs. This presents a significant security risk, as sensitive internal data could be exposed to external threats.
2. **Inadequate Wi-Fi Coverage:**
   - The existing Wi-Fi coverage throughout the building is insufficient. We are currently using a low-cost booster in the office, which is not designed for business use and fails to provide the necessary reliability and performance.
3. **Outdated Access Points:**
   - We have Wi-Fi access points located in the First Floor Server Room and the Garth Room. These older UAP-AC-LR models are no longer optimal for our needs. Their current positioning may also not be ideal for maximum coverage and efficiency.

Recommendations:

1. **Segregate Networks:**
   - Implement separate networks for public and office use. This will enhance security by ensuring that sensitive business data remains protected and isolated from public access. It also allows us to improve our public and guest wifi options for the OCR community and gives us options to host different kinds of events,
2. **Relocate Access Points:**
   - **Move the current access point from the First Floor Server Room to the office** to eliminate the need for the low-cost booster and improve coverage in the office area.
   - **Move the current access point from the Garth Room to the Weir Room** - We will replace the Garth Room with a more updated date, higher capacity access point and allow us to add additional wifi access to the Weir Room
   - **Note on Lift Installation:**
     - With the upcoming lift installation, additional IT might be required to move network equipment, which will change Wi-Fi behaviour around the building. In light of the impending installation of the new elevator, additional information technology support may be necessary to facilitate the relocation of network equipment. Moreover, this

undertaking is likely to result in alterations to the wireless internet connectivity patterns within the building.

3. **Add a New Internet Gateway Cyber Security\Guest Wi-Fi Filtering:**
   ○ Introduce a new internet gateway specifically for the guest Wi-Fi. This will allow us to filter and block inappropriate and dangerous websites, ensuring a safer browsing environment for visitors.
   ○ Implement a splash screen for the guest Wi-Fi network, requiring users to agree to terms and conditions before accessing the internet. This can include policies on acceptable use and disclaimers to protect the venue.
   ○ Posabley Utilise the splash screen for community advertising, promoting upcoming events, services, or important announcements to guests.

Benefits:

- Enhanced security for office data.
- Improved Wi-Fi coverage and reliability.
- Safer internet browsing experience for guests.
- Reporting on usage to gain insight into future decisions.
- Keeping track of how things are used to make better choices in the future.
- Opportunity to communicate directly with the community through the splash screen.

Quoted Costs From Jellyfish IT:

- Ubiquiti UniFi UCG-Ultra Security Cloud Gateway Ultra Security Appliance: £112.74
- Ubiquiti U6-Mesh Wireless 6 Access Point - Garth Room Ground Floor: £170.40
- Ubiquiti In Wall Wireless 6 Access Point - Castle Room 1st Floor: £185.33
- Replacement Switch for Cabinet - Ubiquiti 16 Port Rack Mount PoE: £280.49
- Installation and configuration - Installation and Configuration of Switch, Wireless Points, Security Gateway: £500.00

  Total: £1,248.96