



FREE GUIDE · 2026 EDITION

The Complete Guide to Technology for Leisure and Entertainment Venues in Scotland

A practical guide for venue operators: guest WiFi, card payments and PCI DSS, cyber security, staff communications, multi-site IT and choosing an IT partner.

By Kenny Stevenson, Operations Director · Indigo Unified Communications
Updated September 2026 · indigocomms.co.uk/guides/leisure-technology/

Contents

1. Overview

The Complete Guide to Technology for Leisure and Entertainment Venues in Scotland

2. What are the biggest technology challenges for leisure and entertainment venues?

3. How do you design WiFi and networks for a busy venue?

4. How do venues keep card payments secure and PCI DSS compliant?

5. How should leisure businesses protect customer and booking data?

6. What's the best way for venue staff to communicate?

7. How do you manage IT across several venues?

8. How do you choose an IT provider for a leisure venue?

9. Venue technology readiness checklist

Every chapter is also on our website, where links and sources are kept up to date:
indigocomms.co.uk/guides/leisure-technology/

The Complete Guide to Technology for Leisure and Entertainment Venues in Scotland

Leisure and entertainment venues in Scotland need technology that works hardest when the building is full. Get six things right: a connection sized for your busiest day with automatic backup, WiFi designed for crowds, card payments on their own protected network, cyber security that protects booking and customer data, communications that reach staff on the floor, and one standard across every site. This guide explains each in practical terms.

Who this guide is for

It's written for owners, general managers, operations and duty managers and finance leads at Scottish music and events venues, football and sports clubs, stadiums, family entertainment and soft play centres, attractions and multi-site leisure operators.

Why technology matters more than ever in leisure

The visitor economy is a big part of Scotland's economy. VisitScotland reports £10.8 billion of visitor spending in 2023, 239,000 people employed in tourism in 2024, and 16,325 registered tourism businesses, 97% of them small (Scottish Growth Sector Statistics, December 2025).

Almost all of that spending now goes through technology. Cash made up just 9% of UK payments in 2024, while debit cards made up 53% and contactless 39% (UK Finance, 2025). Tickets are scanned from phones, bookings are taken online and CCTV runs over the network. When the connection drops on a sold-out night, it isn't an IT problem. The bars, gates and box office all stop at once.

Two deadlines add pressure. The UK's analogue phone network closes on 31 January 2027, which affects some card machines, alarms and lift lines, and PCI DSS v4.0.1 is now the only version of the card security standard in force.

What's in this guide

1. **What are the biggest technology challenges for leisure and entertainment venues?** The eight problems we see most, from peak-time demand to staff turnover.
2. **How do you design WiFi and networks for a busy venue?** Capacity, segmentation, events and stadiums.

3. **How do venues keep card payments secure and PCI DSS compliant?** Card terminals, EPOS, network separation and the PSTN switch-off.
4. **How should leisure businesses protect customer and booking data?** Cyber Essentials, ticketing data and UK GDPR.
5. **What's the best way for venue staff to communicate?** Phones, radios, mobiles and Teams.
6. **How do you manage IT across several venues?** One standard for every site, including CCTV and access control networks.
7. **How do you choose an IT provider for a leisure venue?** Questions to ask before you sign.
8. **Venue technology readiness checklist** 20 yes/no questions to test where you stand.

The guide at a glance

A modern venue technology setup focuses on:

- A connection sized for the busiest event, with automatic failover
- High-density WiFi, with guests, staff, tills, ticketing and CCTV on separate networks
- Card payments protected in line with PCI DSS v4.0.1
- Every line checked before the PSTN switch-off
- Cyber security that protects booking and customer data
- Staff accounts and devices that can be set up and removed quickly
- One standard, managed centrally, across every site

The biggest misconception we come across

How Indigo does this. Many venues assume a faster internet line will fix a busy-night problem. Usually it won't. The failures we see come from everything sharing one flat network: guest phones, tills, ticket scanners and cameras all competing for the same WiFi. At Indigo Unified Communications, from our base in Glasgow, we support SWG3, Falkirk Football Club and Wonderworld Group's 10 sites, and the first fix is nearly always separating those systems and sizing for the peak, not the average.

Frequently asked questions

What IT does a leisure or entertainment venue need?

Most venues need a business connection with automatic backup, WiFi designed for crowds, a separate secure network for tills and card payments, managed devices for staff, and a phone system that copes with busy booking periods. Behind that sits the same Microsoft 365, cyber security and helpdesk support as any other business.

Does our venue need to comply with PCI DSS?

Yes. Any business that accepts card payments must protect card data under the Payment Card Industry Data Security Standard. Version 4.0.1 has been the only active version since 31 December 2024. Your acquirer, the bank that processes your card payments, tells you how to show compliance. For most venues that means a self-assessment questionnaire.

Will the PSTN switch-off affect our card machines and alarms?

It might. The UK's analogue phone network closes on 31 January 2027, and Openreach has named payment terminals, alarms and lift emergency phones as particular risks. Anything still using an analogue line needs moving to a digital service. A free [PSTN switch-off check](#) will show what's affected.

Where to start

Start with a structured review of your current setup, looked at through the lens of your busiest day. It shows the risks, quick wins and longer-term improvements before you commit to new systems or suppliers. See also our [leisure and entertainment sector page](#).

Sources: VisitScotland, *Scotland's Visitor Economy* (Scottish Growth Sector Statistics, December 2025), <https://www.visitscotland.org/research-insights/latest-research/visitor-economy> · UK Finance, *UK Payment Markets 2025* summary (October 2025), <https://www.ukfinance.org.uk/system/files/2025-10/Payment%20Markets%20Report%20Summary.pdf> · PCI Security Standards Council, *Just Published: PCI DSS v4.0.1*, 11 June 2024, <https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1> · ISPreview, *Openreach confirm post-January 2027 measures for UK analogue phone switch-off*, 24 September 2026, <https://www.ispreview.co.uk/index.php/2026/09/openreach-confirm-post-january-2027-measures-for-uk-analogue-phone-switch-off.html>

[Book a free Venue Technology Assessment](#) →

What are the biggest technology challenges for leisure and entertainment venues?

The eight technology challenges we see most in Scottish leisure and entertainment venues are: peak-time demand, card payment security, guest WiFi, the PSTN switch-off, customer and booking data, staff turnover, missed booking calls, and keeping several sites consistent. They usually share one cause: systems added one at a time, by different suppliers, all running on the same network and nobody looking at the whole picture.

1. Peak-time demand

An office network copes with the same people every day. A venue has to cope with a sold-out gig, a match day or the first day of the school holidays. That's when thousands of phones, card terminals, ticket scanners and cameras compete for the same connection, and it's exactly when nothing can fail.

Best practice: size the connection and WiFi for your busiest event, with automatic failover. See Chapter 2.

2. Card payment security

Cash made up only 9% of UK payments in 2024 (UK Finance, 2025), so a venue that can't take cards can't trade. Tills and card terminals must be protected under PCI DSS, and they shouldn't share a network with guest WiFi.

Best practice: put payment systems on their own protected network. See Chapter 3.

3. Guest WiFi that fails when the venue is full

Customers expect WiFi to work, and many venues rely on it for app-based ordering, digital tickets and social media. WiFi designed for floor area rather than people collapses on the busiest night.

Best practice: design for density, with fair-use limits per guest.

4. The PSTN switch-off

The UK's analogue phone network closes on 31 January 2027. Around 350,000 business premises still hadn't moved by September 2026 (Openreach, via ISPreview). In venues, it isn't just the

phones. Older card machines, intruder and fire alarms, lift emergency phones and door entry can all rely on an analogue line.

Best practice: list every line and every device that uses one, and move them before the deadline. Use our free PSTN switch-off check.

5. Customer and booking data

Ticketing, bookings, memberships, parties and mailing lists all hold personal data. Across UK businesses, 43% reported a breach or attack in the last 12 months (Cyber Security Breaches Survey 2026). A breach means reporting duties under UK GDPR as well as lost trust.

Best practice: protect accounts with multi-factor authentication and work towards Cyber Essentials. See Chapter 4.

6. Staff turnover and shared devices

Seasonal, part-time and event staff need access quickly and need removing just as quickly, often on shared tills and tablets. Shared passwords and ex-staff with live accounts are common weak points.

Best practice: individual logins, centrally managed devices and a simple starter and leaver process.

7. Missed booking calls

Parties, functions, hospitality packages and group bookings still often start with a phone call. Calls missed in busy periods are lost revenue.

Best practice: a cloud phone system with call queues, out-of-hours messages and reporting. See Chapter 5.

8. Keeping several sites consistent

Operators with several venues often find every site set up differently, with different suppliers, passwords and equipment. Problems take longer to fix and costs are hard to see.

Best practice: one standard site build, managed centrally. See Chapter 6.

What these challenges have in common

They look different, but most come down to one thing: tills, ticketing, CCTV, door entry, guest WiFi and back-office systems were added one at a time, often by different suppliers, onto one network. Nobody owns the whole picture until something fails on a busy night.

How Indigo does this. Indigo Unified Communications supports the systems venues depend on: EPOS and tills, ticketing and booking systems, CCTV networks, and door entry and access control. We keep each on its own secure network, monitor them from our Glasgow base, and work directly with your EPOS or ticketing provider when a fault is inside their software, so you have one number to call.

Sources: UK Finance, *UK Payment Markets 2025* summary (October 2025) · ISPreview, *Openreach confirm post-January 2027 measures for UK analogue phone switch-off*, 24 September 2026, <https://www.ispreview.co.uk/index.php/2026/09/openreach-confirm-post-january-2027-measures-for-uk-analogue-phone-switch-off.html> · DSIT, *Cyber Security Breaches Survey 2025/2026*, 30 April 2026.

Book a free Venue Technology Assessment →

How do you design WiFi and networks for a busy venue?

Design venue WiFi for the number of people in the space on your busiest day, not for floor area. That means enough access points in the right places, limits on how much each guest can use, and a connection sized for peak demand with automatic 4G/5G failover. Keep guests, staff, tills, ticketing and CCTV on separate networks, so a packed guest network can't slow down payments or entry.

Why venue networks are different

In an office, a few dozen people use the network in a predictable way. In a venue, the number of people can go from a handful to several thousand in an hour, and they all arrive with phones. At the same moment, card terminals, ticket scanners, CCTV and the box office are working their hardest. A network that feels fine on a quiet Tuesday can fail at 8pm on a Saturday.

How to plan WiFi capacity

Start with a site survey. It should cover:

- **Peak occupancy** in each space, not just the building capacity
- **How people move**, such as queues at the gates, bars at half-time or a packed main room
- **Building materials**, because concrete, steel and glass all block signal
- **What runs over WiFi**: guest access, handheld tills, ticket scanners, staff tablets, streaming
- **Outdoor areas**, stands, car parks and temporary event spaces

From that, the design sets the number and placement of access points, the channel plan (so neighbouring access points don't interfere), and per-guest bandwidth limits so one person streaming can't slow down everyone else.

Why every system needs its own network

The most important design decision is separation. We recommend at least five separate networks (VLANs), each with its own rules:

Network	Who uses it	Why keep it separate
Payments	Tills, card terminals, EPOS	Protects card data and reduces PCI DSS scope
Ticketing and entry	Scanners, box office, turnstiles	Entry keeps working when guest WiFi is busy
Staff	Laptops, tablets, back office	Staff systems stay private
Security	CCTV, door entry, access control	Cameras use a lot of bandwidth and must be protected
Guests	Customers' phones	Isolated from everything else, with fair-use limits

Payments and ticketing get priority over guest traffic. A problem on the guest network, whether it's congestion or a compromised phone, then can't reach the tills.

How much internet does a venue need?

It depends on capacity and what runs over the line. Most venues of any size suit a leased line, which gives the same upload and download speeds and a guaranteed fix time, with a 4G or 5G router that takes over automatically if the main line fails. Check mobile coverage at the exact venue first: Ofcom reports Scotland has the lowest 4G geographic coverage of any UK nation (Connected Nations 2025).

Preparing for events and match days

- Test the network under load before a big event, not during it
- Check failover works by actually switching it
- Agree who to call, and when, if something goes wrong on the night
- Plan temporary areas, such as fan zones or outdoor stages, weeks ahead

What's different about stadium WiFi?

Stadiums pack thousands of people into stands, where the crowd itself absorbs signal. Stadium WiFi needs directional access points, careful channel planning, fair-use limits and a connection sized for match-day crowds, as well as separate networks for club staff, operations and guests.

Frequently asked questions

Is free guest WiFi worth providing?

For most venues, yes. Customers expect it, and it supports digital tickets, app ordering and social sharing. It only helps if it works when the venue is full, so it needs designing for density and keeping separate from your business systems.

Can we use the same WiFi for guests and staff?

You can use the same access points, but not the same network. Each group should have its own network with its own password or login and rules, so guests can never see staff systems, tills or cameras.

How Indigo does this. Indigo Unified Communications designs venue networks on Ubiquiti UniFi, with separate networks for guests, staff, payments, ticketing and CCTV. We delivered a stadium WiFi, connectivity and telephony upgrade for [Falkirk Football Club](#), and we manage WiFi across all 10 [Wonderworld Group](#) sites from one central controller. Every connection is monitored 24/7, and leased lines on fibre Ethernet have a 5-hour fix time. Out-of-hours and event-day engineer cover is available by arrangement, from our Glasgow team. More on our [venue WiFi and connectivity](#) and [business WiFi](#) pages.

Sources: Ofcom, *Connected Nations: Nations report 2025* (Scotland), 19 November 2025, <https://www.ofcom.org.uk/phones-and-broadband/coverage-and-speeds/nations-report-2025> · PCI Security Standards Council, *Payment Card Industry Data Security Standard v4.0.1*, June 2024, https://www.pcisecuritystandards.org/document_library/

[Book a free Venue Technology Assessment →](#)

How do venues keep card payments secure and PCI DSS compliant?

Venues keep card payments secure by putting tills, EPOS and card terminals on their own protected network, away from guest WiFi, staff devices and CCTV. That reduces how much of the venue falls under PCI DSS v4.0.1, the card security standard every card-accepting business must follow. Use terminals your payment provider supports, remove default passwords, keep software updated, and check no card machine still relies on an analogue phone line before 31 January 2027.

What is PCI DSS, and does it apply to us?

The Payment Card Industry Data Security Standard (PCI DSS) is the security standard for any business that stores, processes or transmits card data. If your venue takes card payments, it applies to you, whatever your size.

Version 4.0.1 was published in June 2024, and version 4.0 was retired on 31 December 2024, leaving 4.0.1 as the only active version. The 51 "future-dated" requirements in version 4 became mandatory on 31 March 2025 (PCI Security Standards Council).

How you prove compliance is set by your acquirer, the bank or payment provider that processes your card payments. For most venues, that's an annual self-assessment questionnaire (SAQ). Which SAQ you complete depends on how your payments are set up, and a simpler setup means a shorter questionnaire.

Why network separation matters most

PCI DSS applies to every system that handles card data and every system connected to it. If your tills share a flat network with guest WiFi, office PCs and CCTV, all of those can fall into scope. The PCI Security Standards Council doesn't require network segmentation, but it strongly recommends it, because it's the most effective way to reduce scope, cost and risk.

In practice, that means:

- A dedicated network for tills, EPOS and card terminals
- A firewall between the payment network and everything else, allowing only the traffic payments need
- Guest WiFi completely isolated from payments
- The separation tested regularly, as PCI DSS requires where segmentation is used to reduce scope

Card terminals and EPOS: the basics

- **Use terminals from your payment provider** and keep them on its supported list
- **Consider point-to-point encryption (P2PE).** A validated P2PE solution encrypts card data inside the terminal and can greatly reduce what you need to evidence. Ask your payment provider
- **Change default passwords** on EPOS, routers and back-office systems
- **Give every member of staff their own login** on the EPOS, not a shared code
- **Keep software updated** on tills, terminals and the back office
- **Check terminals for tampering**, especially at busy, unattended or temporary points of sale
- **Keep a list** of every device that takes payments and where it is

How does the PSTN switch-off affect card machines?

Some older card machines still dial out over an analogue phone line. So can intruder and fire alarms, lift emergency phones and door entry. The UK's analogue network closes on 31 January 2027.

Openreach confirmed in September 2026 that lines still on the old network will move to a temporary "emergency voice access" service, from £35 a month per line wholesale (retail prices will be higher), and that migrations with broadband attached won't start until mid-April 2027. Around 350,000 business premises still hadn't moved, and Openreach named payment terminals, alarms and lift emergency phones as particular risks (ISPreview, 24 September 2026).

Emergency voice access is a stopgap. Move card machines to an IP or mobile (SIM) connection now, and check each alarm and lift line with its supplier.

Frequently asked questions

Do mobile card readers need to be on the venue WiFi?

Not always. Many portable terminals connect over their own mobile SIM, which keeps them off your network entirely. If they use WiFi, they should join the payment network only, never the guest or staff network.

Can Indigo make our venue PCI compliant?

We build and manage the network separation, firewalls, device security and monitoring that PCI DSS expects. The compliance assessment itself stays between you and your acquirer, and we can provide the network information your self-assessment questionnaire asks for.

How Indigo does this. Indigo Unified Communications puts tills, EPOS and card terminals on their own protected UniFi network at every venue we support, including SWG3 in Glasgow, so busy nights on the guest WiFi don't affect the bars. We check every phone line, alarm, lift line and card machine as part of our free PSTN switch-off check and plan the move to digital. See how we support venue systems on our [IT support for venues page](#).

Sources: PCI Security Standards Council, *Just Published: PCI DSS v4.0.1*, 11 June 2024, <https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1> · PCI Security Standards Council, *Now is the Time for Organizations to Adopt the Future-Dated Requirements of PCI DSS v4.x*, 20 August 2024, <https://blog.pcisecuritystandards.org/now-is-the-time-for-organizations-to-adopt-the-future-dated-requirements-of-pci-dss-v4-x> · ISPreview, *Openreach confirm post-January 2027 measures for UK analogue phone switch-off*, 24 September 2026.

[Book a free Venue Technology Assessment →](#)

How should leisure businesses protect customer and booking data?

Leisure businesses protect customer and booking data with the basics done consistently: multi-factor authentication on every account, especially ticketing, booking and email; individual logins for every member of staff; managed, updated devices; email filtering; tested backups; and a quick leaver process for seasonal and event staff. Cyber Essentials covers most of this and proves it to partners and insurers. Know your UK GDPR duty to report serious breaches within 72 hours.

What data does a venue hold?

More than most people think. Ticketing and booking systems hold names, email addresses, phone numbers and purchase history. Memberships and season tickets add dates of birth and payment details. Party bookings can include children's names and ages. Then there's CCTV footage, staff records and supplier bank details. All of it is personal data under UK GDPR, and much of it sits in cloud systems that are only as secure as the passwords protecting them.

How venues are attacked

Across UK businesses, 43% reported a breach or attack in the last 12 months, and phishing was by far the most common, affecting 38% (Cyber Security Breaches Survey 2026). For venues, the usual patterns are:

- **Phishing** that steals a manager's email or ticketing login
- **Payment fraud**, where a fake supplier or promoter email changes bank details
- **Account takeover** of booking platforms, social media or email marketing tools
- **Ex-staff** whose accounts were never switched off
- **Shared passwords** on tills, tablets and back-office systems

The protections every venue needs

Identity

Multi-factor authentication on email, ticketing, booking, EPOS back office, social media and banking. Only 47% of UK businesses use two-factor authentication (Cyber Security Breaches Survey 2026), so this is the single biggest quick win.

Starters and leavers

Every member of staff gets their own login, with access only to what their role needs. When they leave, or when the season ends, access is removed the same day.

Devices

Laptops, tablets and phones centrally managed, encrypted and updated, with endpoint protection. Shared devices locked down to the apps staff need.

Email

Filtering for phishing and impersonation, and a rule that any change to supplier or promoter bank details is confirmed by phone on a known number.

Backup and recovery

Microsoft 365 and key systems backed up, and recovery tested. Ask your ticketing and booking providers how they back up your data too.

Is Cyber Essentials worth it for a venue?

For most venues, yes. It's the government-backed scheme covering five controls: firewalls, secure configuration, user access control, malware protection and software updates. Corporate clients, event partners and public bodies increasingly ask for it, and the NCSC reports certified organisations are 92% less likely to claim on their cyber insurance. Only 5% of UK businesses hold it (Cyber Security Breaches Survey 2026). Smaller operators can start with the NCSC's free Cyber Action Toolkit, launched in October 2025, which leads towards Cyber Essentials.

What if something goes wrong?

Under UK GDPR, a personal data breach that's likely to put people at risk must be reported to the ICO within 72 hours of you becoming aware of it. Have a short incident plan: who decides, who calls your IT provider, who contacts the ICO and how you'll tell customers.

Frequently asked questions

Who is responsible for data held in our ticketing platform?

Usually you are, as the data controller, even when the platform provider stores it. Check your contract with the provider, turn on multi-factor authentication for every user, and remove access for staff who leave.

Do seasonal staff need their own accounts?

Yes. Shared logins make it impossible to know who did what, and they can't be switched off when one person leaves. Individual accounts, set up and removed quickly, are safer and are expected under Cyber Essentials.

How Indigo does this. Indigo Unified Communications holds Cyber Essentials Plus and ISO 27001:2022 itself. Every client gets Kaseya 365 endpoint protection, INKY email security and multi-factor authentication, with Microsoft Intune managing staff and shared devices. Our Platinum package adds a 24/7 security operations centre (RocketCyber) and includes Cyber Essentials support, which any business can also buy separately. Our Glasgow team handles starters and leavers so seasonal staff are set up and removed quickly.

Sources: DSIT, *Cyber Security Breaches Survey 2025/2026*, 30 April 2026 · Infosecurity Magazine, *Cyber Essentials Has Record Year*, 17 September 2026, <https://www.infosecurity-magazine.com/news/cyber-essentials-has-record-year/> · NCSC, *Small businesses to receive cyber security boost with new toolkit from experts*, 14 October 2025, <https://www.ncsc.gov.uk/news/small-businesses-receive-cyber-security-boost-with-new-toolkit-from-experts> · ICO, *Personal data breaches: a guide*, <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/>

[Book a free Venue Technology Assessment →](#)

What's the best way for venue staff to communicate?

Most venues need three layers: a cloud phone system for bookings and enquiries, with call queues and out-of-hours messages; instant, hands-free communication on the floor, usually two-way radios; and managed business mobiles for duty managers and event teams. Microsoft Teams ties the office together. With the analogue phone network closing on 31 January 2027, any venue still on old lines needs to move now.

Booking calls: the revenue you can't see

Parties, functions, hospitality packages and group bookings often start with a phone call, and they tend to come in when staff are busiest. A missed call rarely rings back. A cloud phone system helps by:

- **Queuing calls** and ringing several people at once, on desk phones, laptops or mobiles
- **Routing calls by time**, so out-of-hours callers hear opening times and a booking link
- **Reporting** on missed calls and busy periods, so you can staff the phones properly
- **Keeping your numbers** when you move, since numbers can be ported to a new system

Radios or mobiles on the floor?

It isn't usually one or the other.

	Two-way radios	Business mobiles
Best for	Instant, one-to-many talk on the floor: security, stewards, bar and floor staff	Duty managers, event teams, anyone who moves between sites or calls out
Strengths	Push a button and everyone hears it; works when mobile signal is poor inside the building	Calls, messages, email, apps and Teams; reaches anyone, anywhere
Watch out for	No record or reach beyond the venue; batteries and chargers to manage	Coverage inside large buildings; needs central management

Many venues use radios for live operations and mobiles for managers. Some add push-to-talk apps to business mobiles, which can suit smaller teams where signal is good. Check mobile coverage inside the building before relying on phones: concrete stands and basements often block signal.

Business mobiles for venue teams

Treat mobiles as operational equipment, not perks. Buy centrally, choose the network by checking coverage at each venue, enrol every phone in mobile device management so it can be wiped if lost, and review the bill regularly. Rugged handsets suit outdoor, stadium and warehouse staff.

Microsoft Teams for the back office

Teams gives office, marketing, events and finance staff chat, meetings and shared files in one place. With Teams Phone, it can also carry your phone numbers, so managers take booking calls on a laptop or mobile wherever they are.

Don't forget the PSTN switch-off

The UK's analogue phone network closes on 31 January 2027. That affects old phone systems and ISDN, and also card machines, alarms, lift emergency phones and door entry that use an analogue line. Run our free PSTN switch-off check to see what needs to move.

Frequently asked questions

What phone system suits a leisure venue?

A cloud phone system with call queues, out-of-hours routing and reporting suits most venues. The right platform depends on call volumes, how many sites you have and whether you already use Microsoft Teams. Fully hosted systems start from about £10 per user per month for a single handset.

Can we switch phone systems without disrupting the venue?

Yes. New phones can be installed during working hours and run alongside the old system, so there's no downtime. Number transfers are scheduled by Openreach between 9am and 5pm.

How Indigo does this. Indigo Unified Communications supports 8x8, 3CX and Microsoft Teams Phone, so we recommend the platform that fits your venue rather than one product, and every review prices both hosted and SIP options. We supply business mobiles on EE, O2 and Vodafone, managed with Microsoft Intune, and we've been the official mobile supplier to Celtic Football Club since March 2022. Our Glasgow team sends a phone system review within 2 working days. See our leisure sector page.

Sources: ISPreview, *Openreach confirm post-January 2027 measures for UK analogue phone switch-off*, 24 September 2026 · Celtic FC, *New official mobile supplier to the club*, 1 March 2022, <https://www.celticfc.com/news/2022/march/01/new-official-mobile-supplier-to-the-club/>

Book a free Venue Technology Assessment →

How do you manage IT across several venues?

Manage several venues by giving every site the same standard build: the same connectivity with automatic failover, the same WiFi and network layout, the same separate networks for tills, CCTV and door entry, and the same managed devices. Manage it all centrally, so head office can see every site, changes roll out once, and most faults are fixed remotely. New and temporary sites then go live quickly, on a known design.

Why multi-site IT goes wrong

Most multi-site operators grow one venue at a time. Each site gets whatever the local supplier installed at the time, so after a few years there are different routers, WiFi, passwords, phone contracts and CCTV setups at every location. Nobody has a complete list of what's where. Every fault needs someone on site, and head office can't see which sites are at risk.

What a standard site build includes

Layer	Standard
Connectivity	Full fibre or leased line, with 4G/5G failover
Network	The same firewall, switches and separate networks at every site
WiFi	The same access points and settings, managed from one controller
Payments	Tills and terminals on their own protected network
Security systems	CCTV, door entry and access control on their own network
Devices	Laptops, tablets and phones managed centrally
Phones	One cloud phone system across all sites, with site-specific call routing
Documentation	Every site's equipment, lines and passwords recorded in one place

CCTV, door entry and access control

These systems are often installed by security contractors and plugged into whatever network is there. That causes two problems. Cameras send a lot of video, which can slow the network on a busy day, and poorly secured cameras and recorders are a common way in for attackers.

Put them on their own network, change default passwords, keep firmware updated, and control who can view footage remotely. CCTV footage of identifiable people is personal data, and the ICO

expects it to be kept secure, with access limited to the people who need it. Agree with your security contractor who is responsible for the cameras and who is responsible for the network they sit on.

Connecting the sites together

Head office often needs to reach systems at every site, and sites need to reach central systems. Software-defined networking (SD-WAN or SASE) connects the sites securely, applies the same security rules everywhere and shows performance at every site from one place.

Temporary sites, pop-ups and events

For festivals, fan zones, pop-ups or a site waiting for a fixed line, a managed 4G/5G router can get a venue online in days. Check coverage at the exact location first: Ofcom reports Scotland has the lowest 4G geographic coverage of any UK nation, although 5G is available outside 77% of premises (Connected Nations 2025).

Frequently asked questions

How quickly can a new venue be brought online?

With a standard site build, most of the design work is already done. A 4G/5G router can usually get a site live within days while a fixed line is installed. Leased lines take longer, typically 30–90 working days, so order them as early as possible.

Can faults be fixed without sending an engineer?

Many can. When every site's network, WiFi and devices are monitored and managed centrally, engineers can see the fault, restart equipment, change settings and push updates remotely. Site visits are then kept for hardware failures.

How Indigo does this. Indigo Unified Communications provides managed IT support, connectivity, WiFi and phones across all 10 Wonderworld Group sites, with every site on one standard and the WiFi managed from one UniFi controller. We document every site in IT Glue, and manage devices with Microsoft Intune. Managed 4G/5G connections are usually live within 2–3 working days. Our Glasgow team monitors every line 24/7. See IT support for venues.

Sources: Ofcom, *Connected Nations: Nations report 2025* (Scotland), 19 November 2025, <https://www.ofcom.org.uk/phones-and-broadband/coverage-and-speeds/nations-report-2025> · ICO, *Video surveillance (including guidance for organisations using CCTV)*, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/>

[Book a free Venue Technology Assessment →](#)

How do you choose an IT provider for a leisure venue?

Choose a provider with named leisure clients you can check, experience of the systems venues run on (EPOS, ticketing, CCTV and door entry), a clear answer on evening, weekend and event-day cover, and the ability to manage connectivity, WiFi, phones and mobiles as well as IT. Check their published response times and security certifications, and ask the ten questions below before you sign.

Seven things to look for

1. Venue experience you can check

Ask for named leisure clients, case studies and references from venues like yours. A provider that only supports offices may never have planned for a sold-out night.

2. Knowledge of venue systems

Tills, card terminals, ticketing and booking platforms, CCTV, door entry and access control all sit on your network. Your provider should support that network and work with each system's supplier when something breaks, so you don't have to.

3. A clear answer on out-of-hours cover

Your busiest times are evenings, weekends and holidays. Ask exactly what's covered outside office hours: monitoring, alerts, phone support and engineer attendance. Get it in writing, including any extra cost.

4. Security and payments

Ask how they protect card payment networks, whether they can help you towards Cyber Essentials, and how they handle starters and leavers. Check whether they hold Cyber Essentials Plus and ISO 27001 themselves.

5. One team for IT, connectivity and phones

When the internet, WiFi, phones and IT come from different suppliers, each can blame another when something fails on a busy night. One team with real expertise in each area makes faults quicker to fix.

6. Published response times

Ask for their average first response time and resolution rates, and how they're measured.

7. Room to grow

They should support new sites, temporary events, acquisitions and rising security requirements without starting from scratch.

Ten questions to ask an IT provider

1. Which leisure or entertainment venues do you support, and can we speak to one?
2. Do you support the network behind our EPOS, ticketing, CCTV and door entry?
3. What cover do we get in the evenings, at weekends and on event days, and what does it cost?
4. How will you keep card payments separate from guest WiFi?
5. What happens if our internet fails in the middle of an event?
6. How quickly can you set up and remove seasonal staff?
7. Can you manage our WiFi, connectivity, phones and mobiles too?
8. Have you checked our lines for the PSTN switch-off?
9. What certifications do you hold?
10. What does success look like after 12 months?

Signs you've outgrown your current IT provider

- Problems on busy nights aren't picked up until Monday
- Nobody can tell you which systems share the guest WiFi
- Suppliers blame each other when something fails
- Ex-staff still have working logins
- Every site is set up differently
- Nobody has mentioned the PSTN switch-off
- They don't understand how a venue works

Frequently asked questions

Do IT providers offer 24/7 support for venues?

It varies. Many providers, including us, run a daytime helpdesk and add 24/7 monitoring so faults are spotted at any hour. Engineer cover for evenings and events is often arranged separately. Ask exactly what's included and what costs extra.

How Indigo does this. Here are our answers. Indigo Unified Communications supports SWG3, Falkirk Football Club and Wonderworld Group, and we've been Celtic FC's official mobile supplier since 2022. Our helpdesk runs 09:00–17:00 Monday to Friday (08:30–17:30 on Platinum), with 24/7 monitoring on Gold and Platinum, and out-of-hours and event-day engineer cover by arrangement at extra cost. In August 2026 we handled 1,701 tickets with a 28-minute average first response, resolving 63% within two hours. We keep 95% of our clients, score 4.98/5 from post-ticket surveys and hold Cyber Essentials Plus, ISO 27001:2022 and ISO 9001:2015. Read our case studies for [SWG3](#), [Falkirk FC](#) and [Wonderworld](#).

"Since moving to Indigo, Kenny and the team have provided us with a new level of support, comfort, and confidence in our 'round the clock' reliance on IT and connectivity." **Bob Jahavari, Operations Director, SWG3**

Sources: Indigo service desk data, August 2026 · DSIT, *Cyber Security Breaches Survey 2025/2026*, 30 April 2026.

[Book a free Venue Technology Assessment](#) →

Venue technology readiness checklist

Answer these 20 yes/no questions to see whether your venue's technology is ready for its busiest day. They cover connectivity, WiFi and networks, card payments, cyber security, communications and running several sites. If you answer "no" to three or more, there are likely to be quick wins. If you answer "no" to any payments or cyber security question, start there.

Connectivity

1. Is our internet connection sized for our busiest event, not an average day?
2. Does a backup connection take over automatically if the main line fails?
3. Have we tested that failover in the last six months?

WiFi and networks

4. Does our WiFi still work well when the venue is full?
5. Are guests, staff, tills, ticketing and CCTV on separate networks?
6. Does guest WiFi have fair-use limits per person?

Card payments

7. Are tills, EPOS and card terminals on their own protected network?
8. Do we know which PCI DSS self-assessment questionnaire applies to us, and is it up to date?
9. Have default passwords been changed on EPOS, routers and terminals?
10. Have we confirmed no card machine, alarm, lift line or door entry system relies on an analogue phone line before 31 January 2027?

Cyber security

11. Is multi-factor authentication on for email, ticketing, booking and banking?
12. Does every member of staff have their own login, including on the tills?
13. Are leavers' accounts removed on the day they leave?
14. Are our devices centrally managed and updated automatically?
15. Have we achieved, or planned for, Cyber Essentials?
16. Do we know what to do, and who to tell, within 72 hours of a data breach?

Communications

17. Can our phone system queue booking calls and report on missed calls?

18. Are business mobiles centrally managed and able to be wiped if lost?

Several sites and support

19. Is every venue set up to the same standard, with an up-to-date record of equipment and lines?

20. Do we know exactly what IT cover we have in the evenings, at weekends and on event days?

What next?

A "no" isn't a failure. It's a list of what to fix first, starting with payments and cyber security. If you answered "no" to several questions, a structured review will show the risks, quick wins and longer-term improvements before your next big event. Indigo Unified Communications reviews connectivity, WiFi, payment networks, phones and IT support for venues across Scotland from our Glasgow office, and we'll show you where the risks are on your busiest day.

Sources: PCI Security Standards Council, *Just Published: PCI DSS v4.0.1*, 11 June 2024 · ISPreview, *Openreach confirm post-January 2027 measures for UK analogue phone switch-off*, 24 September 2026 · ICO, *Personal data breaches: a guide*.

[Book a free Venue Technology Assessment →](#)

Back to: [The Complete Guide to Technology for Leisure and Entertainment Venues in Scotland](#)

Talk to Indigo

Indigo Unified Communications provides managed IT support, cyber security, connectivity, phone systems and business mobiles to organisations across Scotland, from offices in Glasgow and Livingston. We hold Cyber Essentials Plus, ISO 27001:2022 and ISO 9001:2015.

Book a free technology assessment: 0141 442 0202 ·
gethelp@indigocomms.co.uk · indigocomms.co.uk/contact/

Indigo Unified Communications is a trading name of Indigo E-Commerce Digital Limited, registered in Scotland, company number SC599200. Information correct at September 2026; this guide is general guidance, not professional advice for your specific situation.