



FREE GUIDE · 2026 EDITION

The Complete Guide to Technology for Renewable Energy Companies in Scotland

A practical guide for Scottish solar, battery storage and renewables firms: remote site connectivity, cyber security, field mobiles, Microsoft 365 and AI.

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

Contents

1. Overview

The Complete Guide to Technology for Renewable Energy Companies in Scotland

2. What are the biggest technology challenges for renewable energy companies?

3. What does a good IT strategy look like for a renewable energy business?

4. How should renewable energy companies protect themselves from cyber attacks?

5. What's the best internet for a remote solar or battery storage site?

6. What mobile technology do renewables field teams need?

7. How can renewable energy companies get more from Microsoft 365 and AI?

8. How do you choose an IT provider for a renewable energy company?

9. Renewable energy technology readiness checklist

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

The Complete Guide to Technology for Renewable Energy Companies in Scotland

Renewable energy companies in Scotland need technology that works across an office, remote sites and field teams. Get five things right: reliable connectivity at every site, managed and secure devices for engineers, cyber security that meets developer and utility supply chain requirements such as Cyber Essentials, a clear line between business IT and site control systems, and a roadmap that keeps up with project-driven growth. This guide explains each one in practical terms.

Who this guide is for

It's written for owners, managing directors, operations and project managers, office managers and finance directors of Scottish renewable energy businesses: solar and battery storage companies, installers and contractors, and developers and consultancies. Most have a head office, several sites and people spread across Scotland.

It's written by Indigo Unified Communications, a Glasgow-based managed IT, connectivity, cyber security and business mobiles provider supporting more than 10 renewable energy businesses.

Why technology matters more than ever in renewables

The sector is growing quickly, and much of that growth is in the places technology struggles to reach. At the end of March 2026, Scotland had 22 operational battery storage projects with an estimated 843 MW of capacity, and 32.8 GW of battery storage in the planning pipeline (Scottish Government, June 2026).

Every project brings new sites, people, devices and data. Rural sites are hard to connect: 4G from all mobile operators covers only 67% of Scotland's landmass, the lowest of any UK nation (Ofcom, 2025). And 43% of UK businesses reported a breach or attack in the last 12 months (DSIT, April 2026), and larger developers and utilities now ask their suppliers to prove their security before awarding work.

What's in this guide

1. **What are the biggest technology challenges for renewable energy companies?** The eight problems we see most.
2. **What does a good IT strategy look like for a renewable energy business?** Six pillars, a technology stack and a roadmap.

3. **How should renewable energy companies protect themselves from cyber attacks?** Cyber Essentials and keeping business IT apart from site systems.
4. **What's the best internet for a remote solar or battery storage site?** 4G, 5G, satellite, fixed lines and failover compared.
5. **What mobile technology do renewables field teams need?** Networks, rugged devices, Intune and lone working.
6. **How can renewable energy companies get more from Microsoft 365 and AI?** Project workspaces and Copilot.
7. **How do you choose an IT provider for a renewable energy company?** Ten questions to ask.
8. **Renewable energy technology readiness checklist** 20 yes/no questions to test where you stand.

The biggest misconception we come across

How Indigo does this. Many renewables businesses assume their technology problems are about the sites. In our experience, most start in the office: unmanaged laptops, shared logins to monitoring portals, project files in personal inboxes and no plan for the next site. We support more than 10 renewable energy businesses from Glasgow, and the biggest gains usually come from managing every device through Microsoft Intune, turning on multi-factor authentication and giving each project a proper home in Teams and SharePoint.

Frequently asked questions

What IT does a small renewable energy company need?

At minimum: Microsoft 365 with multi-factor authentication on every account, managed and encrypted laptops and phones, endpoint protection, email security, Microsoft 365 backup and a reliable connection at the office and each site. Add Cyber Essentials if you supply developers, utilities or the public sector. Most small solar and battery storage firms can run all of this on Microsoft 365 Business Premium.

How do you get internet to a remote solar or battery storage site?

Start with a coverage check at the exact location across EE, O2 and Vodafone. Most sites can be connected with a 4G or 5G router and an external antenna, often within days. Where mobile coverage is too weak, low-orbit satellite works almost anywhere. Long-term sites can add a fixed line, with the mobile or satellite link kept as automatic backup.

Do renewable energy suppliers need Cyber Essentials?

Increasingly, yes. Developers, utilities and public bodies ask suppliers and subcontractors to show cyber security controls, and Cyber Essentials is the most common baseline. It's required for central government contracts that involve personal data or OFFICIAL information (PPN 09/23). Only 5% of UK businesses hold it (DSIT, April 2026), so certification also helps a firm stand out.

Should our IT provider manage our inverter or battery monitoring systems?

Not usually. Inverter, battery and grid control systems are normally specified and supported by the equipment provider or grid operator. Your IT provider should manage business IT, keep it separate from those systems, and secure the laptops, phones and accounts your engineers use to reach monitoring portals. Indigo Unified Communications works this way and doesn't manage SCADA.

Where to start

Start with a structured review of your current setup. It shows the risks and quick wins before you commit to new systems or suppliers.

Sources: Scottish Government, *Energy Statistics for Scotland – Q1 2026*, 30 June 2026, <https://www.gov.scot/publications/energy-statistics-for-scotland-q1-2026/> · Ofcom, *Connected Nations 2025: Scotland report*, 19 November 2025, <https://www.ofcom.org.uk/phones-and-broadband/coverage-and-speeds/nations-report-2025> · DSIT, *Cyber Security Breaches Survey 2025/2026*, 30 April 2026, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026>

[Book a free Renewable Energy Technology Assessment](#) →

What are the biggest technology challenges for renewable energy companies?

The eight technology challenges we see most in Scottish renewable energy companies are: connecting remote sites, equipping field teams, supply chain cyber requirements, keeping business IT apart from site control systems, onboarding for new projects, protecting project data, too many suppliers, and uncertainty about AI. They usually share one cause: technology added project by project instead of planned.

1. Connecting remote and rural sites

Solar farms and battery storage sites are built where land and grid capacity are available, not where broadband is. Fixed lines can be miles away, and 4G from all mobile operators covers only 67% of Scotland's landmass, the lowest of any UK nation (Ofcom, 2025). Site cabins still need drawings, permits, cameras and Teams calls.

Best practice: a connectivity plan for every site, based on a coverage check at the exact location. See Chapter 4.

2. Equipping field teams

Installers and engineers work on rooftops, in fields and at substations. Their phones and tablets hold site photos, drawings, permits and customer details, and they get dropped, rained on and lost.

Best practice: rugged devices where needed, the network with the best coverage at your sites, and every device centrally managed. See Chapter 5.

3. Supply chain cyber requirements

Developers, utilities and public bodies increasingly ask subcontractors and consultants to show security controls, usually starting with Cyber Essentials. Yet only 15% of UK businesses review the cyber risks posed by their own immediate suppliers (DSIT, April 2026), so the pressure mostly comes from the top of the chain down.

Best practice: treat Cyber Essentials as a condition of winning work. See Chapter 3.

4. Keeping business IT apart from site systems

Inverters, battery management systems and monitoring platforms are increasingly connected. If they share a network, or login details, with office laptops, a problem in one can spread to the other.

Best practice: separate networks, separate accounts, and clear responsibility for each side.

5. Onboarding for new projects

Renewables businesses grow in bursts. A new project can bring new starters, contractors and devices at a few weeks' notice, and when it ends, access has to be removed just as quickly.

Best practice: standard devices configured in advance through Microsoft Intune, and a written process for joiners and leavers.

6. Protecting project and commercial data

Grid applications, site designs, landowner agreements, planning documents and financial models are valuable and confidential. They're often shared with partners, consultants and investors by email attachment, with no control over where copies end up.

Best practice: one secure place for project documents, with controlled external sharing. See Chapter 6.

7. Too many suppliers

Many firms end up with separate providers for IT, broadband, site routers, phones and mobiles. When something fails at a remote site, nobody owns the problem.

Best practice: fewer suppliers and one roadmap. See Chapter 2.

8. Uncertainty about AI

We hear the same questions often. Is Microsoft Copilot worth it? Is our data safe? The opportunity is real, but only with clear objectives and sensible rules.

Best practice: start with practical uses that save time on reports and admin.

Frequently asked questions

What's the most common technology problem for solar and battery storage companies?

Connectivity at remote sites is the problem we're asked about most. Sites are chosen for land and grid access, not broadband, and rural mobile coverage in Scotland varies widely by network. A coverage check at the exact location, a managed 4G or 5G router and a backup connection solve most cases.

Why do renewables businesses struggle with IT as they grow?

Because growth comes in bursts tied to projects. Setups that work for 15 people break at 50, especially when new starters and contractors arrive at short notice. Standard devices, central management through Microsoft Intune and a joiners and leavers process let a business add people in days without losing control.

How Indigo does this. Indigo Unified Communications supports more than 10 renewable energy businesses from Glasgow, including solar and battery storage companies, installers and developers. The pattern we see most is a business that grew project by project: a router bought for one site, a phone contract for another, laptops set up by whoever joined first. We start by putting all of it on one list, then fix the risks before adding anything new.

Sources: Ofcom, *Connected Nations 2025: Scotland report*, 19 November 2025, <https://www.ofcom.org.uk/phones-and-broadband/coverage-and-speeds/nations-report-2025> · DSIT, *Cyber Security Breaches Survey 2025/2026*, 30 April 2026, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026>

[Book a free Renewable Energy Technology Assessment →](#)

What does a good IT strategy look like for a renewable energy business?

A good IT strategy for a renewable energy business is built around projects and sites, not just the office. It rests on six pillars: connectivity planned for every site, managed devices for field teams, cyber security that meets supply chain requirements, a clear boundary with site control systems, secure project collaboration and a roadmap tied to the project pipeline. It's delivered in three phases: stabilise, modernise and optimise.

Why renewables needs a different IT strategy

A typical office business has one location and a stable headcount. A solar, battery storage or renewables business may have a head office, several live sites, engineers on the road, contractors joining for one project, and partners who need access to some documents but not others. The strategy has to work for all of them.

The six pillars

1. Connectivity planned for every site

Every site gets a plan before it's needed: a coverage check, the main connection, failover if the site can't be left offline, and a way to recover the equipment when the project ends.

2. Managed devices for field teams

A standard set of laptops, tablets and phones, including rugged devices where needed, all enrolled in central management so they're encrypted, updated and able to be wiped if lost.

3. Cyber security that meets supply chain requirements

Multi-factor authentication, endpoint protection, email security, backup and monitoring, with Cyber Essentials as the minimum you can show to a developer or utility.

4. A clear boundary with site control systems

Business IT and inverter, battery or grid control systems sit on separate networks, with separate accounts. Everyone knows who owns each side, including the equipment provider.

5. Secure project collaboration

Each project has one home for documents and conversations, with version control and controlled sharing for partners, consultants and investors.

6. A roadmap tied to the project pipeline

New projects mean new sites, people and devices. A roadmap that follows the pipeline means connectivity is ordered in time and new starters have a laptop on day one.

What technology stack do we recommend?

Business need	Recommended approach
Productivity	Microsoft 365 Business Premium
Collaboration	Microsoft Teams and SharePoint, one workspace per project
Device management	Microsoft Intune
Cyber security	Endpoint detection and response, email security and a security operations centre
Backup	Microsoft 365 backup and a tested recovery plan
Office connectivity	Full fibre or a leased line
Site connectivity	4G/5G, satellite where coverage is poor, and automatic failover
Mobiles	Network chosen by coverage at your sites, rugged devices for field teams
Telephony	A cloud phone system that works with Teams and mobiles
AI	Microsoft Copilot where there's a clear use case

The products matter less than making every decision part of one plan.

Signs your IT strategy needs reviewing

- Each new site gets whatever connection someone can find
- Engineers use personal phones for site photos and customer data
- Monitoring portal logins are shared between staff
- New starters wait days for a working laptop
- Project documents live in email attachments
- Nobody has reviewed your technology in the last two years
- A developer or utility has asked for Cyber Essentials and you don't have it

How to build a roadmap in three phases

1. **Stabilise.** Fix recurring issues, turn on multi-factor authentication, enrol every device in management and document every site connection.
2. **Modernise.** Move project files into SharePoint, standardise site connectivity and failover, and achieve Cyber Essentials.
3. **Optimise.** Automate onboarding and approvals, introduce Copilot for reporting, and review the roadmap against the pipeline every quarter.

Frequently asked questions

How often should a renewable energy business review its IT strategy?

At least once a year, and whenever the project pipeline changes significantly. A quarterly check against upcoming projects is better, because site connectivity and new devices need ordering in advance. Leased lines, for example, typically take 30 to 90 working days to install.

Is Microsoft 365 Business Premium enough for a renewables business?

For most businesses of 10 to 300 users, yes. It combines email, Teams, SharePoint, Intune device management and Microsoft's business-grade security features in one subscription. Specialist design, monitoring and financial software sits alongside it, but Business Premium usually covers the core.

How Indigo does this. Indigo Unified Communications starts every engagement by mapping how your people work across the office, sites and the road. Our Platinum package includes Microsoft 365 Business Premium and a 24/7 security operations centre, and onboarding a new client usually takes about two weeks. From our Glasgow office, we then build the roadmap around your project pipeline and review it with you regularly.

Sources: Microsoft, *Microsoft 365 Business Premium service description*, <https://learn.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/microsoft-365-business-premium> · NCSC, *Cyber Essentials: Requirements for IT infrastructure*, <https://www.ncsc.gov.uk/cyberessentials/overview>

[Book a free Renewable Energy Technology Assessment →](#)

How should renewable energy companies protect themselves from cyber attacks?

Renewable energy companies should protect themselves in layers: multi-factor authentication on every account, including monitoring portals; managed and encrypted devices; email security; tested backups; and 24/7 monitoring. Keep business IT on a separate network from inverter, battery and grid control systems. And get Cyber Essentials, because developers, utilities and public bodies increasingly ask for it before awarding work.

Why are renewable energy companies targeted?

Most attacks on smaller renewables businesses aren't sophisticated. They're the same phishing and invoice fraud every business faces: 43% of UK businesses reported a breach or attack in the last 12 months, and phishing was the most common, at 38% (DSIT, April 2026). What makes renewables firms attractive is what they hold and who they work for: grid applications, site designs, landowner agreements, investor models and supplier bank details, and a place in the supply chain of larger developers and utilities.

What supply chain requirements should you expect?

Larger developers, utilities and public bodies increasingly ask suppliers and subcontractors about cyber security in pre-qualification questionnaires. The most common baseline is Cyber Essentials. Under PPN 09/23, it's required for central government contracts that involve personal data or OFFICIAL information.

Cyber Essentials covers five controls: firewalls, secure configuration, user access control, malware protection and software updates. Only 5% of UK businesses hold it (DSIT, April 2026), although 61,430 certificates were issued in the year to June 2026, a record. The NCSC reports certified organisations are 92% less likely to claim on their cyber insurance.

How do you keep business IT separate from site systems?

Inverters, battery management systems and site monitoring are operational technology (OT). They're usually specified and supported by the equipment provider or grid operator, not by your IT provider. But they meet your business IT in two places: the network, and the people who log in.

In January 2026 the NCSC and international partners published eight principles for connecting operational technology securely. For a smaller solar or battery business, the practical points are:

- **Limit exposure.** Site equipment shouldn't be reachable from the internet unless it has to be, and only through the equipment provider's secure route.
- **Keep networks separate.** Office laptops, guest WiFi and site cameras don't share a network with control equipment.
- **Control remote access.** Know which third parties can connect to site systems, how, and remove access when contracts end.
- **Log and monitor.** Record who connects and when.
- **Plan to isolate.** Know how to disconnect a site quickly if something goes wrong.

The people side is where business IT matters most. Staff often reach cloud monitoring portals from ordinary laptops and phones, sometimes with one shared login. Give every person their own account, turn on multi-factor authentication wherever the portal supports it, and make sure the devices they use are managed and up to date.

The layers of protection every renewables business needs

- **Identity:** multi-factor authentication for every user. Only 47% of UK businesses use it (DSIT, April 2026).
- **Devices:** every laptop, tablet and phone encrypted, updated, centrally managed and running endpoint protection.
- **Email:** filtering against phishing and impersonation. Confirm any change of bank details by phone.
- **Data:** project files stored centrally, backed up and tested.
- **Monitoring:** ideally a 24/7 security operations centre.
- **People:** regular awareness training on phishing and invoice fraud.

Frequently asked questions

Is Cyber Essentials enough for a renewable energy supplier?

For most small and medium renewables businesses, Cyber Essentials is the right starting point and often all a developer or utility asks for. Some larger clients ask for Cyber Essentials Plus, which adds an independent technical audit, or ask questions about ISO 27001. Check each client's pre-qualification requirements before you bid.

Who is responsible for securing inverter and battery monitoring systems?

Usually the equipment provider or the operator of the site, under their own contract. Your business is responsible for its own side: keeping your network separate, controlling who has login details, using multi-factor authentication and securing the devices staff use to reach monitoring portals. Agree responsibilities in writing.

How Indigo does this. Indigo Unified Communications holds Cyber Essentials Plus and ISO 27001:2022 ourselves. Every client gets endpoint detection and response (Kaseya 365 Endpoint), INKY email security and Microsoft 365 backup, and our Platinum package adds a 24/7 security operations centre (RocketCyber). We take renewables clients through Cyber Essentials from our Glasgow office. We don't manage SCADA, inverter or battery control systems, but we keep your business network separate from them and work alongside your equipment provider where the two meet.

Sources: DSIT, *Cyber Security Breaches Survey 2025/2026*, 30 April 2026, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026> · NCSC and partners, *Secure Connectivity Principles for Operational Technology (OT)*, January 2026, <https://www.ncsc.gov.uk/files/ncsc-secure-connectivity-for-operational-technology.pdf> · Cabinet Office, *PPN 09/23: Updates to the Cyber Essentials Scheme*, <https://www.gov.uk/government/publications/ppn-0923-updates-to-the-cyber-essentials-scheme> · Infosecurity Magazine, *Cyber Essentials Has Record Year*, 17 September 2026, <https://www.infosecurity-magazine.com/news/cyber-essentials-has-record-year/>

[Book a free Renewable Energy Technology Assessment →](#)

What's the best internet for a remote solar or battery storage site?

For most remote solar and battery storage sites, the best option is a 4G or 5G router with an external antenna on whichever network is strongest at that exact location. Where mobile coverage is too weak, low-orbit satellite works almost anywhere. Long-term sites can add a fixed line, with the mobile or satellite link kept as automatic backup. Always check coverage at the site before committing.

Why remote sites are hard to connect

Solar farms and battery storage sites are chosen for land and grid access. The nearest fixed line can be miles away, and mobile coverage in rural Scotland varies widely by network. 4G from all mobile operators covers 67% of Scotland's landmass, the lowest of any UK nation (Ofcom, July 2025 data). Mobile coverage figures are often quoted for homes and businesses, and a site in the middle of a field can be very different, so national maps are only a starting point.

Which connection should you choose?

Connection	Best for	What to know
4G / 5G router	Construction phase, short projects, backup	Can be live in days. An external antenna and the right network make a large difference
Low-orbit satellite	Sites with little or no mobile signal	Low-orbit services such as Starlink and Eutelsat OneWeb (Indigo supplies both, whichever suits the site) work almost anywhere with a clear view of the sky. Fast enough for cloud apps and video calls in most cases
Fixed broadband (FTTP or SoGEA)	Permanent site buildings near the network	Low monthly cost, but availability at rural sites is limited
Leased line	Offices and large permanent sites	Dedicated bandwidth and a guaranteed fix time. Installation typically takes 30 to 90 working days
Failover	Anywhere downtime is unacceptable	Two different connection types, such as 5G and satellite, so one takes over automatically when the other fails

What does the site actually need the connection for?

Be clear about what the connection is for. During construction, site cabins need drawings, permits, Teams calls, cameras and access to company systems. Once a site is operational, the maintenance team may need a business connection too.

Grid, inverter and battery monitoring links are different. They're usually specified by the equipment provider or grid operator and should stay separate from your business connection. See Chapter 3.

Don't forget the copper switch-off

The UK's copper phone network is being switched off by 31 January 2027. Any office or site still relying on an analogue line, including for alarms, lift lines or older monitoring equipment, needs a plan now.

A site connectivity checklist

- Has coverage been checked at the exact location, on all three networks?
- Is there a backup connection, and does it take over automatically?
- Is site WiFi separate for staff and contractors?
- Can engineers reach company systems securely from the site?
- Is the connection monitored, and who chases the fault?
- What happens to the equipment when construction finishes?

Frequently asked questions

Is satellite internet reliable enough for a solar or battery site?

Modern low-orbit satellite services are fast enough for cloud apps, video calls and cameras at most Scottish sites, and they work where there's no mobile signal. Heavy weather and obstructions can affect them, so for sites that can't be left offline, pair satellite with 4G or 5G to give two independent connections.

How long does it take to connect a new site?

A 4G or 5G router can usually be live within a few working days once coverage is confirmed. A leased line typically takes 30 to 90 working days, so order it as soon as a long-term site is confirmed and use mobile or satellite in the meantime.

How Indigo does this. Indigo Unified Communications checks EE, O2 and Vodafone coverage at the exact site, and our 4G/5G site connections are usually live within 2–3 working days. We offer satellite for remote sites, fixed lines and leased lines (5-hour fix on fibre Ethernet), and automatic failover between two connection types. Our Glasgow engineers monitor every connection we manage and chase the faults for you. See [remote site connectivity for renewables and business connectivity](#).

Sources: Ofcom, *Connected Nations 2025: Scotland report*, 19 November 2025, <https://www.ofcom.org.uk/phones-and-broadband/coverage-and-speeds/nations-report-2025> · Openreach, *Time for a big switch-up as PSTN switch-off looms*, 5 February 2026, <https://www.openreach.com/news/time-for-a-big-switch-up-as-pstn-switch-off-looms/>

[Book a free Renewable Energy Technology Assessment →](#)

What mobile technology do renewables field teams need?

Renewables field teams need phones and tablets on the network with the best coverage at their sites, rugged devices where equipment gets dropped or rained on, and central management through a tool like Microsoft Intune so lost devices can be locked and wiped. They also need a reliable way to stay in touch when working alone, and one business number that reaches them wherever they are.

What's different about field teams in renewables?

Installers and engineers spend their days on rooftops, in fields and at substations, often in rural areas with patchy signal. Their devices hold site drawings, permits, photos, customer details and access to monitoring portals. A wrong network, a cracked screen or a lost phone costs a wasted trip, or worse, a data breach.

Choose the network by coverage, not price

Coverage in rural Scotland varies widely between networks. 4G from all mobile operators covers only 67% of Scotland's landmass (Ofcom, 2025), which means the network that's best in Glasgow may be poor at your sites. Check EE, O2 and Vodafone at the places your teams actually work, and consider mixing networks across teams if your sites are spread out.

Rugged devices

Rugged phones and tablets survive dust, water and drops. They cost more up front but last longer on site. Office staff don't need them, so a mixed fleet usually makes sense.

Manage every device centrally

Every business phone and tablet should be enrolled in mobile device management. With Microsoft Intune, devices are configured before they reach the engineer, company apps and data are kept separate from personal use, updates are enforced, and a lost device can be locked or wiped remotely. When someone leaves, their access goes with them.

If engineers use their own phones, Intune app protection can secure company data in Outlook and Teams without managing the whole device.

Lone working

Many installers and engineers work alone. The HSE says employers must manage the risks before people work alone, including knowing where lone workers are, agreeing regular contact "using phones, radios, email etc", and having devices for raising the alarm. Those systems should be tested regularly.

Technology only helps if it works at the site. Check coverage before relying on a phone-based lone worker app, and have a fallback where signal is weak. There's no single right product: we recommend a lone worker app or device case by case, based on where your people work and the coverage there.

One business number

A cloud phone system lets the office number ring on a desk phone, in Teams or on an engineer's mobile, so customers and site managers reach the right person without personal numbers being shared.

Frequently asked questions

Which mobile network is best for solar installers in Scotland?

It depends entirely on where your sites are. Coverage varies widely by network in rural Scotland, so check EE, O2 and Vodafone at your actual working locations rather than relying on national maps. Some businesses put different teams on different networks to match the areas they cover.

Can we let engineers use their own phones for work?

Yes, with controls. Microsoft Intune app protection keeps company email, Teams and files in managed apps, blocks copying data into personal apps and lets you remove company data without touching personal photos. For engineers who access monitoring portals or customer data, a company-managed device is safer.

How Indigo does this. Indigo Unified Communications supplies business mobiles on EE, O2 and Vodafone, choosing the network by checking coverage at your sites. We're a leading plan.com partner in Scotland, partnered for 10+ years, and plan.com's my.plan app gives you spending caps and user-level controls. We supply a large range of rugged phones and tablets and manage every device through Microsoft Intune from Glasgow. See [business mobiles for renewables field teams](#).

Sources: HSE, *Lone working: training, supervision and monitoring*, <https://www.hse.gov.uk/lone-working/employer/training-supervision-monitoring.htm> · Ofcom, *Connected Nations 2025: Scotland report*, 19 November 2025, <https://www.ofcom.org.uk/phones-and-broadband/coverage-and-speeds/nations-report-2025> · Microsoft, *Microsoft Intune documentation*, <https://learn.microsoft.com/en-us/intune/>

[Book a free Renewable Energy Technology Assessment →](#)

How can renewable energy companies get more from Microsoft 365 and AI?

Most renewable energy companies pay for Microsoft 365 but use little beyond email. The biggest gains come from a Teams and SharePoint workspace for each project, controlled sharing with partners and investors, Intune to manage field devices, and automated approvals. With that in place, Microsoft Copilot can cut time on meeting notes, progress reports and document drafting, with clear rules and a person checking the output.

Why Microsoft 365 suits project-based businesses

Solar, battery storage and renewables businesses run on projects. Each has its own documents, partners, deadlines and confidential information. Microsoft 365 can give every project one secure home that office staff, engineers and approved outsiders can reach from anywhere.

How renewables businesses use each tool

Teams and SharePoint

One workspace per project holds conversations, drawings, grid applications, planning documents, meeting notes and tasks. SharePoint adds version control, permissions and search, so everyone works from the current design. Guest access lets consultants, landowners' agents and investors see only what they need, and you can remove it when the project closes.

OneDrive

Personal working files, synced and recoverable. Project documents belong in SharePoint, not individual OneDrives.

Microsoft Intune

Central management of laptops, tablets and phones: security settings, software, encryption, remote wipe and compliance checks. New starters' devices are ready before they arrive.

Power Automate

Approvals, site sign-offs, expense claims and repetitive data entry can be automated. Small savings repeated across every project add up.

How can renewables businesses use Microsoft Copilot?

Copilot works inside the Microsoft 365 apps your people already use, and respects the permissions you've set. Practical uses:

- **Meetings:** summaries and actions from project and client calls
- **Reports:** first drafts of progress reports, site visit notes and client updates, always checked by a competent person
- **Documents:** summarising long planning, grid or technical documents, and comparing versions
- **Email:** catching up on long threads after days on site

How to use AI responsibly

Copilot can only find what a user already has access to, so sort out permissions first. Otherwise it may surface a financial model or landowner agreement to someone who shouldn't see it. Then agree an acceptable use policy, train staff, and make sure a person reviews anything AI produces before it goes to a client, investor or regulator.

Frequently asked questions

Is Microsoft Copilot worth it for a small renewables business?

It can be, for staff who write lots of reports, attend frequent project meetings or handle long technical documents. Start with a small pilot group, measure the time saved on specific tasks, and fix SharePoint permissions before rolling it out. For staff mostly working on site, the value is usually lower.

How do we share project documents securely with partners and investors?

Use SharePoint or Teams guest access instead of email attachments. You control who sees each folder, can see who opened what, and can remove access when a project or relationship ends. Combine it with multi-factor authentication for guests and sensitivity labels on confidential files.

How Indigo does this. Before anyone buys more software, we review how well a business uses the Microsoft 365 it already has. Indigo Unified Communications is a Microsoft Solutions Partner for Modern Work with more than 100 Microsoft 365 migrations completed. For renewables clients, we set up Teams and SharePoint per project with secure sharing for partners and contractors, protect it with Datto SaaS Protection backup, and manage devices through Intune from our Glasgow office.

Sources: Microsoft, *Microsoft 365 Copilot overview*, <https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-overview> · Microsoft, *Microsoft Intune documentation*, <https://learn.microsoft.com/en-us/intune/>

Book a free Renewable Energy Technology Assessment →

How do you choose an IT provider for a renewable energy company?

Choose a provider that has renewable energy clients, can connect remote sites as well as offices, holds recognised security certifications such as Cyber Essentials Plus and ISO 27001, can manage IT, connectivity and mobiles together, publishes its response times and is clear about where its responsibility ends and your equipment provider's begins. Compare value and outcomes, not just the monthly price.

Seven things to look for

1. Renewables experience

Remote sites, field engineers, project-based growth and supply chain requirements are problems office-only providers rarely see. Ask how many renewables clients they support and what kind.

2. Remote site connectivity

Can they check coverage at your sites, supply 4G, 5G and satellite, set up failover and monitor it? Ask how quickly they can connect a new site.

3. Security they practise themselves

Ask whether they hold Cyber Essentials Plus and ISO 27001, and whether they can take you through Cyber Essentials. A provider that can't pass the audits itself will struggle to get you through them.

4. A clear boundary with site systems

A good provider tells you plainly what they will and won't manage. Be wary of anyone who offers to take over inverter, battery or grid control systems without the specialist expertise and agreement of the equipment provider.

5. IT, connectivity and mobiles together

Separate suppliers for IT, broadband, site routers and mobiles mean nobody owns a fault at a remote site. One provider covering them, with real expertise in each, simplifies support.

6. Published response times

Ask for their average first response and their resolution figures, and how they measure satisfaction.

7. Room to grow

They should be able to onboard new starters and sites quickly and plan around your project pipeline.

Ten questions to ask

1. How many renewable energy businesses do you support?
2. How do you connect a site with poor mobile coverage?
3. How quickly can you get a new site online?
4. Do you hold Cyber Essentials Plus and ISO 27001?
5. Can you take us through Cyber Essentials?
6. What will you manage, and what won't you, at our sites?
7. How do you manage field devices and lost phones?
8. What's your average first response time?
9. Can you manage our mobiles, connectivity and phones too?
10. How often will you review our roadmap against our project pipeline?

Signs you've outgrown your current provider

- Each new site is a scramble
- They can't help when a developer asks for Cyber Essentials
- Field devices aren't managed
- You chase them for ticket updates
- Suppliers blame each other when a site goes offline
- There's no roadmap

Frequently asked questions

Should a renewables business use a specialist or a general IT provider?

A general provider with real renewables clients is usually the best fit. Most of what a solar or battery storage business needs is business IT, but remote site connectivity, field devices and supply chain security need experience a purely office-based provider may not have. Ask for the number and type of renewables clients.

What response time should we expect from an IT provider?

Ask for the average first response and how it's measured. A good managed IT provider should respond to most tickets within an hour and publish its actual figures. Check resolution times too, and whether support covers the hours your field teams work.

How Indigo does this. Here are our answers. Indigo Unified Communications supports more than 10 renewable energy businesses. Every ticket gets a first response in under 30 minutes: in August 2026 we handled 1,701 tickets, with a 28-minute average first response and 63% resolved within 2 hours. We hold Cyber Essentials Plus, ISO 27001:2022 and ISO 9001:2015, keep 95% of our clients and score 4.98/5 from post-ticket surveys. We manage IT, connectivity and mobiles from one Glasgow team, and we don't manage SCADA. See IT support for renewable energy.

Sources: DSIT, *Cyber Security Breaches Survey 2025/2026*, 30 April 2026, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026> · Indigo service desk data, August 2026.

[Book a free Renewable Energy Technology Assessment →](#)

Renewable energy technology readiness checklist

Answer these 20 yes/no questions to see how ready your renewable energy business's technology is. They cover strategy, site connectivity, field teams, cyber security, collaboration and AI. If you answer "no" to three or more, there are likely to be quick wins. If you answer "no" to any cyber security question, start there, because those gaps carry the most risk and are often what developers and utilities check first.

Strategy

1. Do we have a documented technology roadmap linked to our project pipeline?
2. Has our technology been reviewed in the last 12 months?
3. Do we know every supplier, contract and renewal date for IT, connectivity and mobiles?

Site connectivity

4. Do we check coverage at the exact location before connecting a new site?
5. Can we get a new site online within a week?
6. Do sites that can't be left offline have automatic failover?
7. Is every site connection monitored, with someone responsible for chasing faults?

Field teams

8. Are all business phones and tablets centrally managed, and can we wipe a lost one remotely?
9. Are our field teams on the network with the best coverage at our sites?
10. Do we have a tested way to stay in touch with lone workers?

Cyber security

11. Is multi-factor authentication enabled for every user, including on monitoring portals?
12. Does every person have their own login, with no shared accounts?
13. Are office IT and site control systems on separate networks?
14. Do we know which third parties can connect to our site systems, and how?
15. Are our backups tested?
16. Do we hold Cyber Essentials, or have a date to achieve it?
17. Do staff get cyber awareness training at least once a year?

Collaboration

18. Does every project have one secure home for its documents, with controlled sharing for partners?

Artificial intelligence

19. Have we identified where AI could save time on reports and admin?
20. Do we have an AI acceptable use policy?

How to score it

- **18–20 "yes"**: you're in good shape. Review again in a year or when your pipeline changes.
- **13–17 "yes"**: solid foundations with some gaps. Fix any cyber security "no" first.
- **12 or fewer "yes"**: a structured review will show where to start.

Frequently asked questions

Which questions matter most?

The cyber security questions, particularly multi-factor authentication, shared accounts and network separation. These are the gaps attackers use most, and they're the controls developers and utilities check in supplier questionnaires. Only 47% of UK businesses use two-factor authentication (DSIT, April 2026), so this is often the quickest win.

How often should we repeat the checklist?

Once a year, and whenever you start a significantly larger project, open a new office or take on a client with new supply chain requirements. The answers change as the business grows.

How Indigo does this. Our free Renewable Energy Technology Assessment covers all six areas of this checklist. Indigo Unified Communications reviews your current IT setup, cyber security, connectivity for offices and sites, Microsoft 365, business continuity, mobiles and field workforce, and your technology roadmap, then gives you a prioritised list of risks and quick wins. We're based in Glasgow and hold Cyber Essentials Plus and ISO 27001:2022.

Sources: DSIT, *Cyber Security Breaches Survey 2025/2026*, 30 April 2026, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026> · NCSC and partners, *Secure Connectivity Principles for Operational Technology (OT)*, January 2026, <https://www.ncsc.gov.uk/files/ncsc-secure-connectivity-for-operational-technology.pdf> · HSE, *Lone working: training, supervision and monitoring*, <https://www.hse.gov.uk/lone-working/employer/training-supervision-monitoring.htm>

[Book a free Renewable Energy Technology Assessment](#) →

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.