SPIRITMEDIA.

Business Continuity Statement and Plan

Issued: August 2026. Next review: August 2027.

1. Purpose

1.1 This document sets out how Spirit Media Scotland maintains service to its clients through disruption, and how we respond when an incident occurs. It is both our client-facing statement and our working plan, owned by the Joint CEOs and reviewed at least annually. It replaces our 2014 Business Continuity Statement in full.

2. Resilience by Design

2.1 Our operating model removes the single points of failure that continuity planning traditionally exists to manage:

- We are fully remote: our people work from separate locations across the country, so no single event - fire, flood, power failure, transport disruption - can remove our workforce or our workplace.
- We hold no office or company network infrastructure. Our systems are cloud services accessed over the internet, resilient across our provider's infrastructure, and protected by multi-factor authentication and the controls in our IT Access Policy.
- Company and client data is backed up separately from our primary cloud platform by a third-party backup service, so the failure or compromise of the primary platform does not mean the loss of our data.
- Leadership is jointly held: either Joint CEO can act with full authority for the business.
- Written handovers are standard practice before any planned absence, so client knowledge does not sit solely in one head.

3. Recovery Objectives

3.1 In a serious disruption, our objective is to restore critical client activity - live campaign management, time-sensitive media bookings and client communication - within two working days, and normal operations within five working days. Time-critical campaign deadlines are prioritised first.

4. The Scenarios We Plan For

4.1 Cloud service outage or failure. We escalate to our IT provider and the platform vendor, monitor restoration, and communicate with clients on any affected deadlines. If the outage is prolonged, data is recoverable from the separate backup service to alternative provision arranged with our IT provider.

4.2 Cyber incident. Our IT provider isolates affected accounts and devices - revoking access and sessions under the IT Access Policy - and we restore clean data from the separate backup. The Joint CEOs assess our data protection obligations, including whether the incident must be reported to the Information Commissioner's Office within 72 hours, and inform any affected clients promptly and honestly.

4.3 Loss of an individual's workspace or connectivity. A home power cut, broadband failure or damaged device affects one person, not the agency. The individual works from an alternative location or connection (including mobile tethering); replacement equipment is arranged through our IT provider; colleagues pick up anything time-critical in the interim.

4.4 Loss of a key person. Our flat structure, shared documentation and handover discipline mean client work can be picked up by colleagues. If a Joint CEO is suddenly unavailable, the other holds full authority and leads the response.

5. Incident Response

5.1 The Joint CEOs lead any incident. Both hold, securely and offline, the contact details needed if our systems are unavailable: all staff (personal phone numbers), our IT provider, key client contacts, and key media-owner contacts for live campaigns. If systems are down, staff are contacted by telephone cascade; client communication is led by the relevant account leads as soon as a channel is established. Every incident is logged, and the response reviewed afterwards so the plan improves.

6. Testing and Review

6.1 Restoration from the separate backup service is tested with our IT provider at least annually, and the offline contact information is verified at the same time. This document is reviewed at least annually by the Joint CEOs, after any incident in which it is invoked, and on any significant change to our systems, suppliers or ways of working.