



ICT INFRASTRUCTURE ENGINEER

BACKGROUND INFORMATION

Avon Fire & Rescue Service (AF&RS) serves the Unitary Authority areas of Bristol, Bath & North East Somerset, North Somerset and South Gloucestershire. It has 21 operational fire stations, together with offices, covering all areas, with its Head Quarters based in Portishead, near Bristol. AF&RS Control Centre, where emergency calls are handled, is situated in Lansdown, near Bath.

With an annual budget of around £50 million, AF&RS delivers a wide range of fire, rescue and community safety services across a geographic area of approximately 514 square miles with a residential population of more than one million people.

AF&RS employs over 800 staff made up of: Service Delivery including whole-time and on-call Firefighters, and staff in its Control Centre, Service Delivery Support, and Corporate Services.

AF&RS is entering a key phase of its digital transformation, building on recent foundational improvements and progressing a programme focused on modern, secure, and resilient technology services.

We are seeking an ICT Infrastructure Engineer to support and maintain a hybrid estate across cloud and on-premise platforms, ensuring performance, availability, and security. The role will also act as an escalation point for Level 1 and 2 engineers, driving effective resolution and continuous improvement.

The role sits within Digital, Data and Technology in the Corporate Services Directorate and reports to the ICT Supervisor.

With effect from July 2023, UK legislation was amended to enable Fire & Rescue Services to undertake standard Disclosure and Barring Service (DBS) checks for all employees. All AF&RS posts therefore require a standard DBS check, with a few defined roles requiring an enhanced DBS check. These DBS checks will be renewed throughout employment. This post is subject to a standard DBS check.

Safeguarding is the duty of every member of staff at AF&RS: as a public authority we have a responsibility to ensure that the adults and children we interact with are kept safe from harm.



Job Description, Core Values and Person Specification

Job Title	ICT Infrastructure Engineer
Post Number	1110
Grade	HAY 7
Duration of Post	Permanent
Hours	37 per week
Directorate	Corporate Services
Unit or Team	Digital, Data & Technology
Reports to (give job title)	ICT Supervisor
Line management or supervisory responsibilities	No
Responsibility for managing a budget	No
Date job was evaluated	18/06/2026

Purpose of Job:

The ICT Infrastructure Engineer is responsible for the stability, security, and continuous improvement of AF&RS's hybrid ICT estate, ensuring that critical systems underpinning operational response and corporate services are resilient, performant, and aligned to organisational priorities.

The role provides technical expertise across cloud and on-premise infrastructure, taking ownership of the support of core platforms including compute, storage, networking, identity, and security services.

A key aspect of the role is to act as an escalation point for Level 1 and Level 2 engineers, resolving complex incidents and problems, reducing recurring issues, and embedding structured root cause analysis and preventative controls.

The postholder will drive operational maturity through standardisation, automation, and proactive monitoring, ensuring services meet defined SLAs and support a consistent, high-quality user experience.

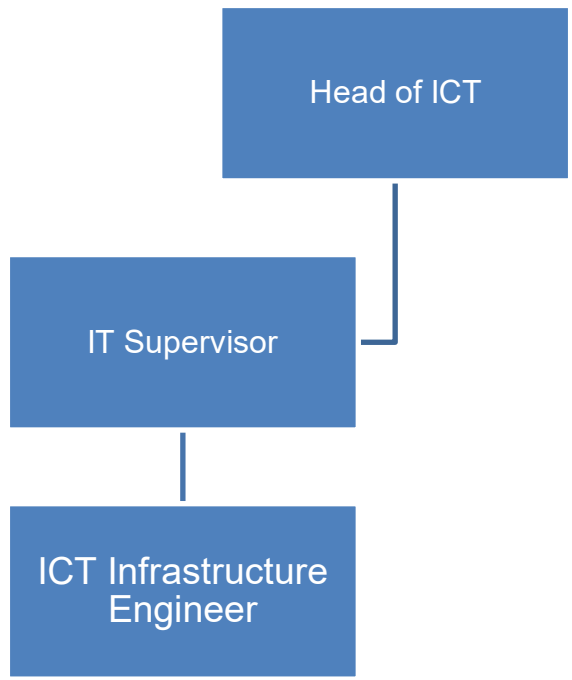
The role plays a central part in AF&RS's transition from outsourced to in-house ICT provision. This includes improving service integration and removing fragmentation across technology domains. The engineer will contribute to building internal capability, establishing robust processes, and ensuring that third-party suppliers are effectively governed and aligned to AF&RS standards.

The postholder is also responsible for maintaining a strong security posture across the infrastructure estate, ensuring alignment with recognised frameworks such as ISO 27001, the NCSC Cyber Assessment Framework, and Cyber Essentials Plus. This includes supporting vulnerability management, patching, identity and access control, logging and monitoring, and incident response readiness.

Working closely with colleagues across Digital, Data and Technology and wider stakeholders, the ICT Infrastructure Engineer will ensure that technology services are reliable, secure, and fit for purpose, directly enabling frontline operations and organisational effectiveness.

This position suits a technically strong, service-focused individual committed to high standards, accountability, and user-centred delivery in support of critical public safety operations.

Structure Chart:



Responsibilities and Duties:

1.	<p>Infrastructure operations (core accountability) Manage the day-to-day operation of the hybrid ICT estate, ensuring the availability, performance, security, and reliability of core services. Monitor system health and capacity, proactively prevent incidents, act as an escalation point for complex technical issues, and drive root cause analysis and resolution. Maintain effective monitoring, alerting, automation, technical documentation, configuration baselines, and support procedures.</p>
2.	<p>Networking (switching, routing, firewalls) Manage and optimise LAN/WAN infrastructure, including switching, routing, firewalls, and site connectivity across MPLS, VPN, internet breakout, and Azure environments. Maintain secure network segmentation aligned to Zero Trust principles, monitor network performance and resilience, troubleshoot complex connectivity issues, and implement firewall, NAT, and access control configurations that support least-privilege access and auditability.</p>
3.	<p>Cloud (Azure) Administer and optimise Azure IaaS and PaaS services, including virtual machines, networking, storage, and backup solutions. Support cloud migration and modernisation initiatives, ensuring secure, resilient, and cost-effective architectures, while maintaining</p>

	governance through policy, tagging, RBAC, and resource standardisation. Monitor performance, availability, disaster recovery, backup, and Azure consumption to drive optimisation and operational resilience.
4.	VMware (on-premise virtualisation) Manage and maintain VMware environments ensuring platform stability, performance, and efficient resource utilisation. Administer the virtual machine lifecycle, maintain backup and failover capabilities, and support integration between on-premise and cloud environments.
5.	Governance and compliance (ISO 27001 / Cyber Essentials Plus) Ensure infrastructure services align with security policies, governance standards, and regulatory requirements, embedding secure-by-design and least-privilege principles throughout the environment. Support the maintenance of the ISMS, participate in audits and assessments, maintain effective configuration and change control, and drive remediation activities arising from findings and risk reviews.
6.	Identity and access (Entra ID / AD DS) Administer and maintain identity services across Entra ID and on-premise Active Directory, supporting user lifecycle management, group policies, and hybrid identity integration. Implement and manage authentication and access controls, including MFA, Conditional Access, RBAC, privileged access management, and device compliance, ensuring secure and effective identity governance across the environment.
7.	Exchange Online administration Administer Exchange Online and associated mail security platforms, managing mail flow, mailbox administration, hybrid configurations, and email security controls including anti-phishing, anti-spam, and transport rules. Troubleshoot mail delivery and access issues, while ensuring compliance with retention, archiving, legal hold, and broader information governance requirements.
8.	Microsoft 365 productivity suite administration Administer core Microsoft 365 services including SharePoint, OneDrive, Teams, and associated collaboration platforms, ensuring secure, reliable, and effective service delivery.
9.	Service improvement and transformation Identify opportunities to standardise, automate, and improve ICT services, contributing to the design and delivery of infrastructure solutions aligned to organisational strategy.
10.	Stakeholder engagement Work collaboratively with internal teams and service users to understand requirements and improve service delivery, providing clear technical guidance to both technical and non-technical stakeholders. Support knowledge sharing and mentoring within the ICT team to strengthen internal capability and promote consistent ways of working.
11.	Cyber security (Microsoft Defender for Endpoint focus) Administer and optimise Microsoft Defender for Endpoint across the server and endpoint estate, ensuring effective protection, detection, response, and vulnerability management capabilities. Monitor and investigate alerts within Defender XDR, support incident response and recovery activities, maintain endpoint security baselines and compliance, and ensure consistent onboarding and health of managed devices. Collaborate with internal ICT teams to remediate security issues, integrate security telemetry into wider monitoring platforms, and continuously improve the organisation's security posture in alignment with recognised frameworks including ISO 27001, NCSC CAF, and Cyber Essentials Plus.
12.	Escalation point

	Act as an escalation point for L1 and L2 engineers, providing technical guidance and support across end-user computing services including Intune, Microsoft Teams, Microsoft 365 productivity applications, and Microsoft Defender technologies.
13.	Carry out any additional responsibilities as reasonable and appropriate, as agreed with line manager.
Special Notes or Conditions:	
1.	<p>AF&RS requires all staff and leaders to promote equality and diversity by:</p> <ul style="list-style-type: none"> ensuring that, both in your dealings with other employees and with members of the public, you comply with all aspects of the Service's Equality Policy and legislation that outlaws discrimination; treating members of the public and other AF&RS staff with respect, dignity and in line with the expectations determined by our Service values at all times; and taking action when witnessing an act that could be considered discrimination or harassment, challenging it and/or raising with managers.
2.	This role is based at Police & Fire HQ in Portishead. Although you are based at a specific location, for efficiency or other business reasons we may require you to travel to and/or work from any base within AF&RS service area or work from home, for which we will pay allowances where appropriate.
3.	If based at Police and Fire Headquarters, this is a secure site and therefore appointment to this post may be subject to passing the required vetting process.
4.	Many posts in AF&RS are hybrid-working with the facility to work from home and from an AF&RS work-base. Your manager will confirm if this applies to this post.
5.	Your job may involve working out of normal office hours, for which mutually agreed compensatory time-off will be given.
6.	Your job may involve you dealing with highly confidential and sensitive information. It is essential that you ensure this information is held and processed securely and that you act with tact and discretion at all times and comply with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Confidentiality must be maintained, even after leaving this post or AF&RS employment.
7.	You should maintain an awareness of environmental regulations in relation to the remit of your role. All employees have a responsibility to carry out their duties in an environmentally conscious way and to actively support AF&RS's Environmental Strategy, Policy and objectives.
8.	You must ensure you maintain an awareness of Health and Safety Regulations relevant to the duties and tasks you carry out and report any situations or incidents which could be considered hazardous. You have a responsibility for your own safety and must not endanger that of colleagues/visitors in the workplace or the public.
9.	There may be times when you are required to wear specific clothing suitable to the type of work you are undertaking. This may include AF&RS branded corporate clothing (for example when representing AF&RS externally), or protective clothing for the work being carried out, as deemed appropriate by your line manager.
10.	All AF&RS posts require a standard DBS check, with a few defined roles requiring an enhanced DBS check. This post is subject to a standard DBS check. These DBS checks will be renewed throughout employment.
11.	Safeguarding is the duty of every member of staff at AF&RS: as a public authority we have a responsibility to ensure that the adults and children we interact with are kept safe from harm.
12.	This role includes participation in a compensated out-of-hours on-call rota for Priority 1 incidents, typically one week in every four.

Avon Fire & Rescue Service Values

We are in the process of embedding the principles of the [Core Code of Ethics](#), on joining the service you will be involved in co-creating what these principles mean to us.

- Putting our communities first
- Integrity
- Dignity and Respect
- Leadership
- Equality, diversity, and inclusion (EDI)

Signed confirmation that this Job Description accurately reflects the requirements of the job:

Job Holder's Manager		Date	
-----------------------------	--	-------------	--

Signed agreement to carry out the responsibilities of this Job Description, and of acceptance of AF&S Values and NFCC Code of Ethics:

Job Holder		Date	
-------------------	--	-------------	--

See following page for Person Specification

Person Specification

Job Title	ICT Infrastructure Engineer			
Post Number	1110			
Grade	HAY 7			
Qualifications, knowledge, experience, skills and personal attributes required for the job:				
	E=Essential D=Desirable	Measured by: A = Application T = Test I = Interview		
		A	T	I
Qualifications/Knowledge				
Degree level education (or equivalent) in computer science or a related field of study, or significant relevant business experience.	E	X		X
Professional ICT qualifications (such as ITIL or accredited status such as Chartered IT Professional CITP), or the equivalent gained through relevant training, experience and continuing professional development.	D	X		X
Up to date technical knowledge of ICT, and the technology landscape, with evidence of keeping up to date with innovations for the benefit of the organisation.	E	X		X
Minimum of 2 years' experience in an Infrastructure Engineer role or similar role.	E	X		X
Experience				
Experience supporting and maintaining a hybrid infrastructure environment (cloud- Azure and on-premise - VMware)	E	X	X	X
Hands on experience administering Azure services (IaaS, networking, identity integration, backup, firewalls, VNETs)	E	X	X	X
Experience managing Active Directory and Entra ID in a hybrid configuration	E	X	X	X
Experience supporting enterprise networking environments (switching, routing, firewalls, VPNs)	E	X	X	X
Experience administering Microsoft 365 services (Intune, Defender, Office 365, Exchange, SharePoint)	E	X	X	X
Experience acting as an escalation point for complex technical issues	E	X	X	X
Experience implementing or maintaining security controls (patching, endpoint protection, access control)	E	X	X	X
Experience with the configuration and management of Meraki firewalls, switches and AP's	D	X		X
Experience working in an environment certified to CE+ or ISO27001	D	X		X

Skills				
Ability to set and manage priorities. Negotiating timescales and balancing work objectives. Delivering effectively, overcoming barriers to change.	E	X		X
Strong problem-solving capability across complex, multi layered environments	E	X		X
Ability to diagnose issues methodically and drive resolution under pressure	E	X		X
Clear technical ownership mindset, taking responsibility for outcomes, not just tasks	E	X		X
Ability to communicate technical issues clearly to non-technical stakeholders	E	X		X
Strong documentation discipline	E	X		X
Ability to automate routine tasks and improve operational efficiency	E	X		X
Ability to challenge poor practices and drive service improvement	E	X		X
Coaching and mentoring capability for junior engineers	E	X		X
Personal Attributes				
Willingness to accept and work to our Values during the course of employment.	E	X		X
Adaptable with a flexible approach to work, to meet business needs.	E	X		X
Able to work effectively both individually and as part of a team.	E	X		X
Professional in conduct.	E	X		X
Strong stakeholder ethics with a customer orientated approach.	E	X		X
Committed to undertake relevant training and continuous professional development opportunities.	E	X		X