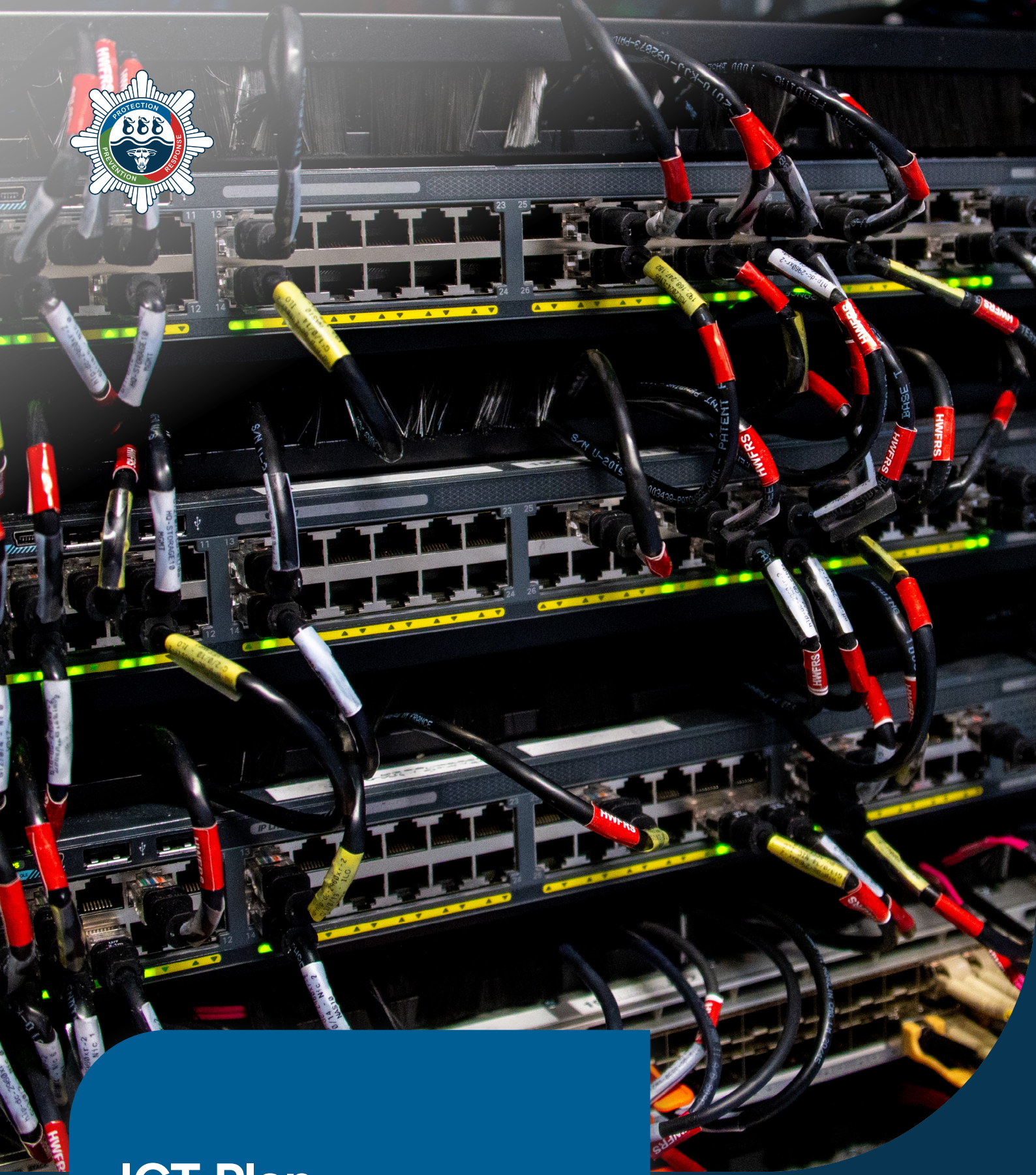


# ICT Plan
2026-30

HEREFORD & WORCESTER
HWFR
FIRE AND RESCUE SERVICE


# Contents



## OUR CORE CODE OF ETHICS

We follow the Core Code of Ethics for Fire and Rescue Services (FRS) in England which guides everything we do.

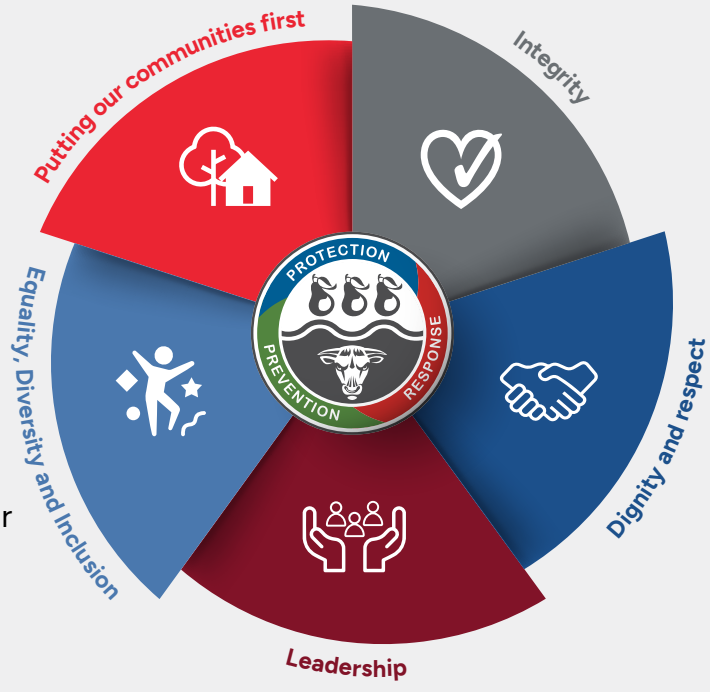
**Putting our communities first**
We put the interest of the public, the community and service users first.

**Integrity**
We act with integrity including being open, honest and consistent in everything we do.

**Dignity and respect**
We make decisions objectively based on evidence, without discrimination or bias.

**Leadership**
As positive role models, we are accountable for everything we do and challenge all behaviour that falls short of the highest standards.

**Equality, Diversity and Inclusion**
We stand against all forms of discrimination, create equal opportunities, promote equality, foster good relations and celebrate difference.




# Introduction

The 2025-30 ICT Plan builds on the successes and lessons of the 2021-25 plan, responding to the evolving needs of Hereford and Worceser Fire and Rescue Service (HWFRS) and the communities it serves. It reflects a commitment to continuous improvement, digital transformation, and alignment with national fire service strategies. The plan is designed to be dynamic, with annual reviews and updates that ensure it remains relevant and responsive to emerging technologies, operational challenges, and legislative changes. The plan aligns to the Digital and Data Strategy 2025-30, supports the new Community Risk Management Plan (CRMP) 2025-30 and integrates with the core strategies of Prevention, Protection, and Response.

This is a key Plan directly linked to the Asset Management Strategy 2025-30.

HWFRS's ICT Vision is to facilitate a digitally empowered fire and rescue service that is agile, inclusive, and data-driven. HWFRS continues to develop a cloud-native architecture with hybrid capabilities, enabling scalable, resilient, and cost-effective infrastructure. This transformation road map will enhance our agility in incident response, will foster inclusivity in both workforce and service design, and empower data-driven decision-making to improve our operational outcomes. HWFRS will harness Artificial Intelligence (AI) technologies to enhance predictive capabilities, automate routine tasks, and personalise service delivery.

HWFRS's ICT Mission is to leverage technology to enhance safety, efficiency, and service delivery across Herefordshire and Worcestershire.

This highlights the central role of ICT in enabling HWFRS to deliver its core services more effectively. By integrating technology into every aspect of operations, from incident response to community engagement, the service can improve safety, reduce risk, and optimise resource use.

HWFRS's ICT Purpose is to support our workforce and communities through innovative, secure, and user-centric ICT solutions. AI will play a key role in streamlining workflows, enhancing decision support, and enabling proactive risk mitigation.

The purpose reflects a dual commitment: empowering staff with tools that make their work easier and more impactful, and ensuring that the public benefits from modern, responsive, and transparent services. ICT will be a key enabler of both internal efficiency and external trust.

# Strategic Approach

Our ICT approach directly supports the three main core strategies: Prevention, Protection and Response, the Service Digital and Data Strategy 2024-30 and the Community Risk Management Plan 2025-30, by maximising the use of digital capabilities to deliver transformation, innovation, resilience and continuous improvement. This includes the following areas:

## A User-Centric Design

Systems and platforms will be designed around the needs of users – whether frontline staff, support teams, or the public. This includes intuitive interfaces, mobile compatibility, and accessibility features that ensure everyone can engage with technology effectively. Regular feedback and usability testing will inform continuous improvements. AI-powered personalisation will be embedded into user interfaces, adapting content and functionality based on user roles and behaviour. Intelligent chatbots and recommendation engines will improve engagement and reduce cognitive load.

## Data Intelligence

HWFRS will invest in advanced analytics tools to transform raw data into actionable insights and meaningful information. Predictive modelling will support risk assessment, resource allocation, and performance monitoring, enabling smarter, faster decisions across the organisation improving performance and productivity.

## Connectivity & Mobility

With an increasingly mobile and distributed workforce, connectivity is critical. The plan will ensure that staff can securely access applications and data from any device, anywhere, using cloud-based platforms with scalable and secure network solutions. This will support agile working and improve core operational responsiveness.

## Cyber Resilience

Cybersecurity will be embedded into every aspect of ICT strategy. HWFRS will adopt a Zero Trust model, implement multi-factor authentication, and maintain compliance with standards such as Cyber Essentials Plus. Regular audits, threat assessments, and staff training will ensure a robust defence against evolving cyber threats. AI-driven threat detection and response systems will be deployed to identify anomalies, automate incident response, and continuously adapt to emerging cyber threats.

# Key Enablers & Targets

## 1 Digital Infrastructure

AI will be used to optimise cloud resource allocation, predict infrastructure failures, and automate system maintenance, ensuring high availability and performance at all times.

## 2 Transition to cloud-native architecture with hybrid capabilities

Moving to a cloud-native infrastructure will provide scalability, resilience, and cost-efficiency. Hybrid models will allow HWFRS to retain control over sensitive data while benefiting from the flexibility and innovation of cloud services. This transition will support disaster recovery, remote access, and will support data classification and data governance and future growth.


## 3 HWFRS will maximise on the use of cellular and mobile networks

The increased performance and wider use of this technology will improve communications, enabling real-time data sharing, high-definition video streaming, and faster access to critical systems. This will enhance situational awareness, improve coordination during incidents, and support advanced applications like drone surveillance and internet sensors.

## 4 Implement Zero Trust Network Access (ZTNA)

ZTNA will replace traditional perimeter-based security with a model that continuously verifies user identity and device health. We will be extending this capability to incorporate Secure Access at the Service Edge (SASE). The use of this technology will extend the network perimeter edge to the end user wherever they are located. This approach will reduce the risk of breaches, especially in remote and mobile environments, and ensure that access to sensitive systems and data is tightly controlled, audited and monitored more accurately.

# Data & Intelligence

## 1 Expand use of Power BI and integrate and further develop AI-driven analytics.

Power BI will be further embedded across departments, enabling staff to create and share interactive dashboards. AI-driven analytics will support predictive maintenance, risk profiling, and performance optimisation, turning raw data into a strategic asset.

## 2 Support a Data Governance Framework.

This framework would define how data is collected, stored, accessed, and used. It will include policies on data quality, security, and compliance, ensuring that all data is trustworthy, protected, and aligned with legal and ethical standards.

## 3 Develop a centralised Data Lake (Data Warehouse) for operational and strategic insights.

A data lake will consolidate information from multiple sources – incident logs, personnel systems, asset databases – into a single, scalable repository. This will support cross-functional analysis, reduce duplication, and enable more comprehensive reporting and planning the aim is to have data models closely linked with AI agents.

## 4 End User Experience.

AI will be used to analyse user behaviour and feedback, enabling dynamic interface adjustments and proactive support. Virtual assistants will further evolve into intelligent agents capable of handling complex queries and learning from each users interactions.

## 5 ICT will start to Roll out AI-powered virtual assistants for internal support such as MS Copilot and others

Virtual assistants will provide instant help with organisational queries, system navigation, and routine tasks, reducing pressure on support teams and improving staff productivity. These tools will learn over time, becoming more effective organisationally whilst providing more personalised and targeted information to our users.

## 6 Enhance mobile-first applications for field operations.

Applications will be redesigned for mobile use, with features tailored to the needs of firefighters and field staff. This includes offline functionality, real-time updates, and integration with GPS and incident management systems.

# Data & Intelligence continued

## 7 Develop regular systematic audits of a product's user experience (UX) and feedback loops.

User experience will be continuously monitored through surveys, analytics, and direct feedback. UX audits will identify pain points and opportunities for improvement, ensuring that systems evolve in line with user needs and expectations.

## 8 Connectivity.

AI-based network monitoring tools will be developed and implemented to predict and resolve connectivity issues, ensuring seamless access and performance across distributed environments.

## 9 Complete digital phone network (PSTN/ISDN) migration.

The transition to digital telephony Session Initiated Protocol will improve call quality, reduce costs, and future-proof communications infrastructure. It will also enable integration with collaboration platforms like Teams, supporting unified communications across the organization.

## 10 Deploy Software-Defined Wide Area Network (SD-WAN) and Secure Access Service Edge (SASE).

SD-WAN will optimise network performance across sites, while SASE will provide secure, cloud-based access to applications. Together, these technologies will support remote work, improve resilience, and simplify network management.

## 11 Integrate multi-factor authentication (MFA) with biometric options.

MFA will be enhanced with biometric verification, such as fingerprint or facial recognition, providing stronger security and a more seamless user experience. This will protect sensitive systems while reducing login friction.

# Digital Culture & Innovation

## 1 Foster a Digital Mindset across all roles.

Staff will be encouraged to embrace technology as a tool for innovation and improvement. We will work across the organisation to establish manual workloads that can be automated with the use of Digital and Data systems. Training, leadership support, and recognition programmes will promote a culture where digital skills and thinking are valued and rewarded. Staff will be introduced to AI concepts and applications relevant to their roles, fostering confidence and curiosity around emerging technologies.

## 2 Promote cross-functional innovation labs.

Innovation labs such as the Data Science and Innovation DSI Pilot Group will bring together staff from different departments to co-design solutions, test new technologies, and share best practices. These labs will act as incubators for ideas that can be scaled across the organisation. Innovation labs will explore AI with data analytics and prediction algorithms for use cases such as automated incident reporting, intelligent resource scheduling, and natural language processing for community engagement.

## 3 Encourage digital upskilling through targeted self-directed learning.

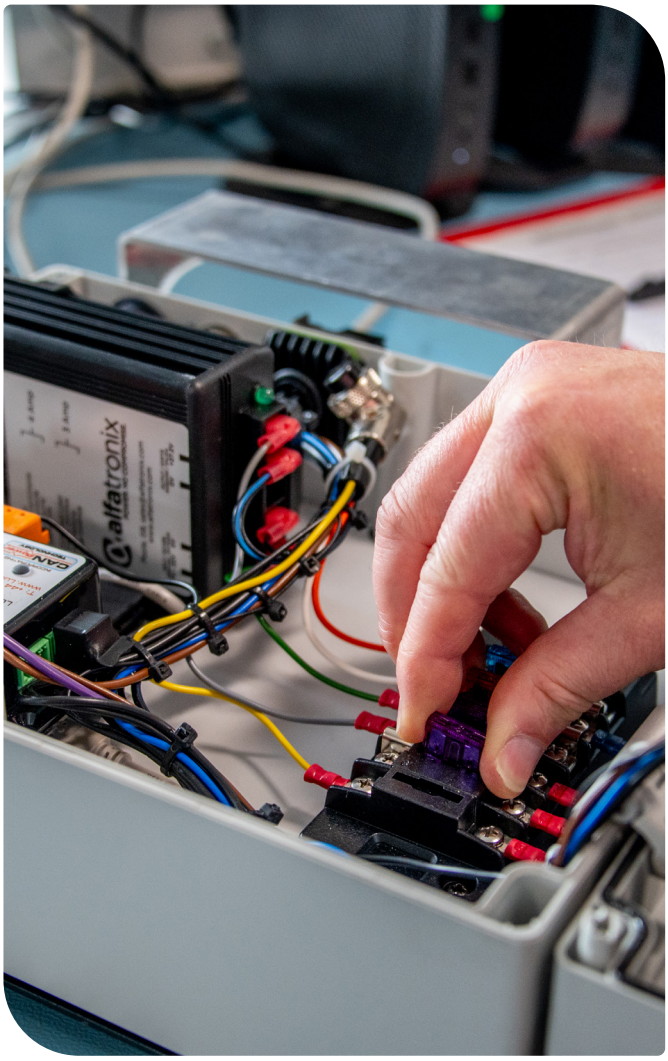
Learning programmes will be accessible to individual staff members to ensure that learning can be tailored to different roles and skill levels, covering everything from basic IT literacy to advanced analytics. Online learning will ensure that all staff can confidently use digital tools.

# Legislative Requirements

## Actual Laws Governing ICT

- The Computer Misuse Act 1990
- The Data Protection Act of 1998
- The Copyright, Designs and Patents Act 1989
- The Health and Safety Act of 1974
- The General Data Protection Regulation 2016
- Data Protection Act of 2018 has been amended to accommodate the post-Brexit changes to UK data privacy law
- UK-GDPR (United Kingdom General Data Protection Regulation) 2020
- UK Data Protection Act 2018 (DPA ACT)
- European VDU & health directive 1992
- Freedom of Information Act 2000
- Online Safety Act 2023
- Data (Use and Access) Act 2025
- Product Security and Telecommunications Infrastructure Act (PSTI) 2022
- Cyber Security and Resilience Bill (expected in late 2025)

Compliance will be maintained through regular audits, policy reviews, and staff training. ICT systems will be designed to meet legal requirements, protect personal data, and support transparency and accountability. This includes adherence to UK-GDPR, the Data Protection Act 2018, Cyber Essentials Plus, and Airwave/ESN Codes of Connection. AI systems will be developed and deployed in compliance with ethical and legal standards, including transparency, explainability, and fairness. HWFRS will adopt responsible AI principles to ensure that automated decisions are auditable and aligned with public trust.



# Monitoring and Review

### 1 Annual reviews aligned with CRMP and Programme of Works:

The ICT Plan will be reviewed annually to assess progress, update priorities, and ensure alignment with the CRMP and other strategic documents. These reviews will be informed by performance data, stakeholder feedback, and emerging trends.

### 2 Develop real-time dashboards for project tracking:

Dashboards will provide visibility into key metrics – such as project status, budget, and impact – enabling proactive management and timely interventions. They will be accessible to leadership and project teams for transparency and accountability.

### 3 Quarterly stakeholder engagement sessions:

Regular engagement with staff and partners will ensure that the ICT strategy reflects diverse perspectives and needs of the organisation. These sessions will be used to share updates, gather feedback, and co-create solutions with the wider teams.

## Strategic Themes Expansion

To further strengthen the strategic themes, HWFRS will adopt a modular approach to digital transformation. Each theme will be supported by dedicated working groups, KPIs, and pilot programs to ensure measurable progress. For example, the 'DSI Group' theme will include quarterly workshops, accessible data, and AI-driven opportunities and AI Agent personalisation trials.

## Performance Monitoring

Real-time dashboards will be developed using Power BI to monitor key metrics such as system uptime, user satisfaction, and response times. Monthly reports will be generated and shared with stakeholders to maintain accountability and drive continuous improvement.

HEREFORD & WORCESTER
HWFR
FIRE AND RESCUE SERVICE

HWFire

**© 2025 Hereford & Worcester Fire and Rescue Service**
Service Headquarters, Hindlip Park, Worcester WR3 8SP
0345 122 4454 | info@hwfire.org.uk | www.hwfire.org.uk