



Digital, Data and Technology Strategy

2027-2030



Contents

Contents	2
Foreword	3
Executive summary	4
Our Purpose and Context.....	5
Our Vision for 2030.....	6
Strategic Objective 1: Better Data and Insight	6
Strategic Objective 2: Simple, Efficient Digital Processes.....	8
Strategic Objective 3: Secure, Reliable and Resilient Technology.....	9
Strategic Objective 4: People and Capability	10
Strategic Objective 5: Focused Innovation and Responsible Use of AI	11
Our Delivery Journey.....	12
Prioritisation and Affordability	13
Governance and Accountability	13
Measuring Success	14
Commitment	14



Foreword

Royal Berkshire Fire and Rescue Service exists to help create safer and more resilient communities. To achieve this, our people need reliable information, dependable systems, secure technology and straightforward ways of working.

This Digital, Data and Technology Strategy sets out how we will use these capabilities over the next three years to make a practical difference: enabling our people to spend less time on avoidable administration, making it easier to access useful information, strengthening our resilience against disruption and helping the Service make better decisions for the communities we serve.

Technology alone will not achieve these outcomes. The value comes from using it purposefully: understanding the risks we are managing, improving the processes that frustrate colleagues today, maintaining high-quality information at the point it is created and investing carefully in the capabilities that matter most.

The strategy is deliberately focused on the period 2027–2030. Technology, operational demands and financial circumstances will continue to change quickly. A three-year strategy gives the Service a clear destination and sufficient time to build lasting capability, while allowing us to review priorities annually and respond to the emerging Community Risk Management Plan, Annual Plan and financial position.



Executive summary

This strategy describes how RBFRS will use digital, data and technology to help our people work more safely, efficiently, and effectively between 2027 and 2030.

Its purpose is not to introduce technology for its own sake. It is to improve the experience of colleagues, strengthen operational and organisational resilience, improve the information available for decision-making and release time and resources for the work that matters most.

By 2030, we want colleagues across RBFRS to experience a Service where:

- » Information is easier to find, understand and use when it is needed.
- » Staff spend less time producing, reconciling and checking manual reports.
- » The data entered into systems has a clear purpose and is used to support real decisions.
- » Leaders can see a consistent picture of performance, risk, demand and delivery.
- » Digital processes are simpler, more joined up and designed around the people who use them.
- » Critical systems are reliable, recoverable and better protected against cyber threats.
- » The Service is more confident that it can continue to operate effectively through disruption.
- » DDaT investment is focused on the greatest contribution to safety, resilience, efficiency, and supports the CRMP.

The strategy makes three principal choices:

1. **Start with the foundations that matter most.** We will understand our current data, process, technology and skills position; identify priority datasets and processes; improve cyber resilience; and establish the minimum standards needed for reliable reporting and delivery.
2. **Focus investment on a manageable number of priorities.** We will not attempt to transform every system, dataset or process at once. We will prioritise the work that improves safety, resilience, efficiency, operational decision-making and value for money.
3. **Deliver benefits early while building for the future.** We will pursue practical improvements from the outset, including reducing manual reporting and simplifying high-value workflows, while creating the capability needed for more



advanced data, automation and innovation later.

The strategy is organised around five strategic objectives:

- » Better data and insight for safer, more informed decisions.
- » Simple, efficient digital processes that improve everyday work.
- » Secure, reliable and resilient technology.
- » People and capability for confident use of DDaT.
- » Focused innovation that delivers practical value.

Detailed actions, milestones, investment requirements, owners, dependencies and measures will be set out in a rolling implementation plan. The strategy sets the direction and the choices; the implementation plan will explain how delivery will happen.

Our Purpose and Context

RBFRS is committed to creating safer and more resilient communities through prevention, protection, response and resilience activity. Digital, data and technology support every part of that purpose.

They help us understand community and operational risk, plan prevention and protection activity, deploy resources, manage people and assets, learn from incidents, maintain assurance, communicate effectively and use public money responsibly.

The Service is also operating in an environment of financial pressure, rising expectations, changing technology and increasing cyber risk. These factors mean we must make disciplined choices. We cannot afford to invest in every opportunity at once, but neither can we afford to under-invest in the systems, information and safeguards that keep the Service functioning.

This strategy will be anchored to the new CRMP as it develops, while not waiting for the CRMP before acting. It will support the Annual Plan and wider corporate priorities by enabling the Service to:

- » Keep people safe through reliable systems, effective information and better-supported decision-making.
- » Keep the organisation safe through cyber resilience, information assurance, sound governance and business continuity.
- » Improve efficiency by reducing manual work, avoiding duplication, simplifying processes and directing investment to areas that deliver tangible benefit.



- » Modernise in a controlled and sustainable way, so that progress is achievable and does not create unnecessary pressure or risk.

Our Vision for 2030

By 2030, RBFRS will be a more digitally enabled and data-informed fire and rescue service.

For a firefighter, manager, support colleague or senior leader, that should feel different in practical ways. Important systems will be more reliable. Information needed to perform a task or make a decision will be easier to access. Colleagues will not have to spend unnecessary time collating spreadsheets, reconciling conflicting reports or re-entering the same information into multiple places.

Digital tools and processes will be clearer and more consistent. People will understand why information is collected and how the quality of that information affects colleagues, operational decisions and the Service's ability to deliver for communities.

For the organisation, this will mean greater confidence in the availability and security of technology, stronger assurance over risks and performance, improved productivity and a more sustainable platform for future change.

Strategic Objective 1: Better Data and Insight

What we are seeking to achieve

Data is valuable only when it helps people understand something, make a decision or take action. Our focus will therefore be on improving the information that matters most to prevention, protection, response, resilience, workforce planning, asset management, finance and organisational performance.

We will use data to help answer practical questions:

- » Where are the risks to our communities and how are they changing?
- » Are our prevention, protection and response activities achieving the intended outcomes?
- » Where are pressures, delays, duplication or avoidable demand occurring?
- » What do we need to know to deploy resources effectively and manage performance confidently?
- » Which investments, process changes or interventions are delivering the greatest benefit?



What will be different

The Service will identify and focus on a limited number of priority datasets. For each priority area, we will clarify:

- » Why the data is collected.
- » What decisions, services or statutory responsibilities it supports.
- » Who uses it and in what form.
- » What good-quality data looks like.
- » Who is responsible for maintaining it at source.
- » How it is made available through agreed reports, dashboards or analysis.

We will improve access to information in ways that are proportionate to need. Not all information needs to be available in real time or to every colleague. The objective is that the right people can access the right information, in the right format, at the right time, with appropriate security and control.

Power BI will become the Service's reporting and visualisation tool for agreed corporate and operational reporting. This will reduce the need for recurring manual reporting, provide a clearer single version of key measures and make insight more accessible to those who need it.

Our approach to quality

High-quality data begins when information is entered or recorded. This is not about suggesting that colleagues have previously worked incorrectly. It is about recognising that as the Service makes greater use of information, the value of accurate, complete and timely data increases.

Everyone involved in creating or maintaining priority data will need to understand its purpose and the difference it makes. Business areas will remain responsible for the information and outcomes they depend upon. Business Information and Systems will provide standards, tools, support and assurance to help make good data easier to create, maintain and use.

Critical activities

During the strategy period, we will:

- » Undertake a discovery phase to understand current data, reporting, systems, skills and dependencies.
- » Identify and agree the priority datasets that will deliver the greatest value to the Service.
- » Define the purpose, ownership, quality expectations and use of each priority dataset.



- » Establish common definitions for strategic measures and reduce inconsistent recurring reporting.
- » Standardise agreed reporting through Power BI and governed data models.
- » Deliver early reductions in manual reporting and spreadsheet-based collation.
- » Build practical data literacy among leaders, managers and colleagues who create, analyse or use information.

Strategic Objective 2: Simple, Efficient Digital Processes

What we are seeking to achieve

The Service will use digital tools to remove friction from everyday work. We will not simply digitise inefficient processes; we will redesign selected processes so that they are easier to complete, more consistent, less repetitive and better aligned to the needs of the people using them.

This is where colleagues should see early, tangible benefit. A priority is to reduce the manual activity that consumes time without adding value: repetitive data entry, duplicated approvals, email-based workarounds, manual collation and reporting, and unnecessary movement of information between systems.

What will be different

By focusing on a small number of high-value processes, we will make it easier for staff to complete routine tasks and spend more time on operational delivery, prevention, protection, learning and other higher-value activity.

A practical “day one” measure of success will be the removal or simplification of manual reports and workflows that colleagues currently have to complete repeatedly. These improvements will demonstrate that DDaT is not an abstract corporate programme but a means of improving the daily experience of people across the Service.

Critical activities

During the strategy period, we will:

- » Identify the processes that create the greatest avoidable effort, delay, duplication or error.
- » Prioritise improvements according to their contribution to safety, efficiency, resilience, CRMP delivery and financial benefit.
- » Redesign selected end-to-end user journeys before introducing technology or automation.



- » Use Microsoft 365 and other approved tools to simplify forms, workflows, collaboration and approvals where this offers a clear benefit.
- » Measure benefits such as time saved, reduced rework, improved quality, improved user experience and cashable savings where achievable.
- » Reuse solutions and standards rather than creating separate local approaches to similar problems. a discovery phase to understand current data, reporting, systems, skills and dependencies.
- » Identify and agree the priority datasets that will deliver the greatest value to the Service.
- » Define the purpose, ownership, quality expectations and use of each priority dataset.
- » Establish common definitions for strategic measures and reduce inconsistent recurring reporting.
- » Standardise agreed reporting through Power BI and governed data models.
- » Deliver early reductions in manual reporting and spreadsheet-based collation.
- » Build practical data literacy among leaders, managers and colleagues who create, analyse or use information.

Strategic Objective 3: Secure, Reliable and Resilient Technology

What we are seeking to achieve

Technology is now fundamental to the Service's ability to operate. Our people must be able to rely on core systems, connectivity, devices and information when they need them. We must also be able to continue operating and recover quickly if technology is disrupted.

Cyber resilience is therefore not a technical issue alone. It protects operational continuity, public confidence, organisational finances, sensitive information and the Service's ability to serve communities.

What will be different

By 2029, the Service will have greater confidence in the stability, availability, recoverability and security of its technology estate. Cyber resilience will be embedded in how we design services, procure technology, manage suppliers and prepare for disruption.

The Service will continue to modernise core technology carefully and sustainably. We will make deliberate decisions about what to retain, improve, replace, simplify or retire,



based on operational need, resilience, risk, affordability and value.

Critical activities

During the strategy period, we will:

- » Strengthen cyber controls, monitoring, response arrangements, backup and recovery testing.
- » Continue to work towards recognised cyber assurance standards and sector expectations.
- » Ensure cyber, privacy and information assurance are considered from the beginning of significant change, procurement and system design.
- » Improve the resilience of critical systems, networks, connectivity and identity management.
- » Maintain a planned approach to lifecycle management for devices, infrastructure and core systems.
- » Manage legacy technology through prioritised renewal, retirement and risk-reduction plans.
- » Strengthen supplier assurance where suppliers handle Service information or provide critical technology.
- » Review the capacity, skills and operating model needed to manage cyber risk sustainably.

Strategic Objective 4: People and Capability

What we are seeking to achieve

DDaT will succeed only if people across the Service can use information and technology with confidence, understand their role in maintaining quality and security, and see how change improves their working lives.

The Service also needs the right level of specialist capability to deliver this strategy. The discovery phase will assess the current DDaT operating model, capacity, skills, technology dependencies and delivery demands. It will identify the capabilities that need to be developed, strengthened, bought in or delivered through partnership.

What will be different

Colleagues will receive practical, role-appropriate support rather than generic expectations. A manager using performance information, a colleague entering operational data, a system owner, a report developer and a senior decision-maker each need different forms of capability and support.

The aim is not to make everyone a specialist. It is to give people enough knowledge,



confidence and clarity to use technology effectively, handle information responsibly, recognise cyber risk and contribute to better data and process quality.

Critical activities

During the strategy period, we will:

- » Complete a DDaT discovery phase covering people, capability, systems, data, processes and delivery capacity.
- » Establish role-based learning and support for digital, data, cyber and responsible AI use.
- » Develop specialist capability in data, reporting, process analysis, cyber and DDaT delivery where required.
- » Build Power BI and data literacy capability in BIS and among key managers and reporting users.
- » Clarify responsibilities between BIS and business areas, recognising that business areas own their outcomes, data and processes.
- » Support adoption through engagement, practical guidance, feedback and visible early improvements.

Strategic Objective 5: Focused Innovation and Responsible Use of AI

What we are seeking to achieve

The Service will use new technology where it offers a practical, safe and affordable improvement to productivity, learning, insight, service quality or resilience. We will avoid innovation for its own sake and will not allow interest in emerging technology to distract from the foundations that the Service must get right.

Artificial intelligence, automation and other emerging tools may offer useful opportunities, particularly for drafting, summarising, searching, knowledge retrieval, analysis support and workflow assistance. Their value depends on clear governance, appropriate data, staff confidence and a demonstrable benefit.

What will be different

The Service will take a measured approach: testing a small number of low-risk, high-value uses, learning from them and scaling only where the benefits are clear and risks are properly managed.

This will allow colleagues to benefit from appropriate innovation now, while recognising that more advanced automation, predictive insight and AI-enabled services require mature data, clear safeguards and sustainable capability.



Critical activities

During the strategy period, we will:

- » Establish principles and guidance for the safe, lawful and responsible use of AI.
- » Identify a small number of practical, low-risk use cases with clear success measures.
- » Use pilots to test value, usability, risk and affordability before making wider commitments.
- » Link more advanced innovation to improvements in data quality, integration, platforms and skills.
- » Keep national guidance, cyber implications and public-sector assurance expectations under review.

Our Delivery Journey

This strategy will be delivered through a phased three-year journey. The sequence is important: we will first establish a clear understanding of our starting point and strengthen essential foundations; then simplify, integrate and scale what works; and finally embed sustainable capability and selectively develop more advanced uses of data and technology.

Phase	Period	Strategic Focus	Expected Outcome
Discover, protect and prioritise	2027–2028	Understand current capability; identify priority datasets and processes; strengthen cyber and resilience; establish reporting standards; deliver early manual-reporting and workflow improvements	A realistic, agreed baseline; clear priorities; early visible benefits; improved assurance
Simplify, integrate and embed	2028–2029	Improve priority data quality; expand Power BI reporting; redesign high-value processes; progress priority technology integration and renewal; develop skills	More consistent information, reduced manual effort, improved user experience and stronger resilience
Optimise and sustain	2029–2030	Embed continuous improvement; extend proven automation and insight; mature the data platform; sustain cyber resilience; strengthen benefits realisation	DDaT operating as a trusted, sustainable enabler of service performance and change



The implementation plan will be reviewed regularly and refreshed annually. It will take account of the emerging CRMP, Annual Plan, financial position, operational demands and lessons from delivery.

Prioritisation and Affordability

The Service will not pursue every opportunity at the same time. Activity will be prioritised according to the extent to which it:

- » Improves safety for staff, communities or operations.
- » Supports delivery of the CRMP and Annual Plan.
- » Protects the Service against cyber, technology, information or continuity risk.
- » Reduces avoidable manual work, duplication or process failure.
- » Improves decision-making, assurance or operational insight.
- » Releases capacity, improves productivity or delivers financial benefit.
- » Is achievable within available capability, capacity, funding and time.

This means that essential cyber resilience, reliable technology, priority data and practical productivity improvements will take precedence over lower-value or less mature opportunities.

Where investment is required, business cases will set out the benefits, costs, risks, dependencies, affordability and expected contribution to Service priorities. The Service will seek cashable savings where they are realistic, while also recognising that some investment is necessary to protect resilience, reduce risk and enable effective delivery.

Governance and Accountability

Governance exists to support delivery, make choices and provide assurance. It should be proportionate and focused on outcomes rather than process.

The Fire Authority will retain strategic oversight of the strategy, receiving annual updates on progress, key risks, major decisions and overall assurance.

Strategic Performance Board will review delivery progress, benefits, risks, performance and priorities on a regular basis. A BIS-led DDaT delivery forum will coordinate the detailed pipeline of work, manage dependencies and escalate issues or decisions where needed.

Business Information and Systems will coordinate DDaT standards, platforms, reporting, specialist advice and delivery support. Business areas will remain



accountable for the services, processes, information and outcomes they own. Named owners will be identified for each agreed priority initiative and dataset.

Detailed governance arrangements, responsibilities, project controls and reporting requirements will be maintained in the implementation plan and supporting operating procedures.

Measuring Success

Success will be measured by the difference this strategy makes, not simply by the number of projects completed or policies introduced.

Measures will include:

- » Reduction in time spent on manual reporting, re-keying and avoidable administration.
- » Improvement in the quality and usability of priority datasets.
- » Adoption and usefulness of agreed reports, dashboards and digital workflows.
- » Evidence that data and insight are informing operational, strategic and resource decisions.
- » Availability, resilience and recoverability of critical technology services.
- » Cyber assurance, training, incident readiness and recovery performance.
- » Improvements in user experience and colleague confidence.
- » Benefits delivered, including productivity gains, cost avoidance and cashable savings where applicable.
- » Progress against CRMP, Annual Plan and other corporate priorities enabled by DDaT. safety for staff, communities or operations.

Commitment

This strategy is a commitment to practical, focused and sustainable improvement. It will help RBFRS become a Service where technology works reliably, information has a clear purpose, processes support rather than frustrate people, cyber resilience is taken seriously and investment is directed to the areas that make the greatest difference.

The outcome we seek is straightforward: a safer, more resilient, more efficient Service in which colleagues are better supported to deliver for the communities of Royal Berkshire.