

evidence

public trust

inquiries

reputation

knowledge

accountability

transparency

If you don't protect
your digital assets,
they can't protect you

Technological obsolescence puts information at risk

Electronic communication is how government does business.

In the last ten years we've embraced a host of new information technologies – emails, Wikis and web pages, complex datasets, Blackberries and Blue Tooth to name but a few – and most civil servants now work electronically without a second thought.

This has brought significant opportunities. But it has also introduced serious risks.

The average life of a piece of digital information is just 5 - 7 years. Vital government information is now becoming unreadable or even unrecoverable because the media it's stored on is deteriorating, hardware and software is no longer in use, or successor products can't read old files. For example, 5¼ inch disks, though commonplace 20 years ago, are now obsolete; cds and dvds have a finite lifespan; software used to view documents, such as WordStar, cannot easily be run on modern machines.

When an electronic record becomes unreadable it is usually lost for good.

That means no access to everything from inquiry findings and evidence in criminal cases, right through to budgetary and pensions information, sensitive foreign policy decisions and the location of buried nuclear waste. If you don't take action there's a real chance you won't be able to access information that's more than 5 - 7 years old.

It will make it very difficult for you to operate accountably and transparently, meet your legal and regulatory requirements, answer parliamentary questions or freedom of information requests or take evidence-based policy decisions.

You might be able to recreate some of the information you've lost, but it's expensive and time-consuming. And, of course, some data simply can't be recreated. How could you replace CCTV images of the 2005 London bombings, or raw scientific data from natural disasters, for example?

The potential damage to government reputation and to public trust is colossal.

You can't afford to take the risk.

Help is at hand

Digital files need active management to ensure that they remain readable over the long term.


That's why the Digital Continuity Project has been set up. Led by The National Archives, the Digital Continuity Project is acting on behalf of government departments to create a shared service solution. With our expertise in managing digital projects, The National Archives is well placed to negotiate the best value deal possible. This expertise was recognised at the 2007 Conservation Awards, where The National Archives won the top award for digital preservation.

Over the next couple of years, the Digital Continuity Project will scope your needs, develop a technical specification, and commission a commercial partner (or partners). The partner will then develop a system that guarantees the long-term security, integrity and readability of your digital assets.

The Digital Continuity Project is strongly supported by government, as part of its Transformational Government agenda. It takes advice and guidance from the Knowledge Council and the Chief Information Officers' Council.

What is digital continuity?

- Digital continuity means protecting your digital files from technological obsolescence.
- It's about making sure your data is migrated to new formats as appropriate.
- It covers the sort of information which you may not need on a daily basis, but which you can't afford to lose.



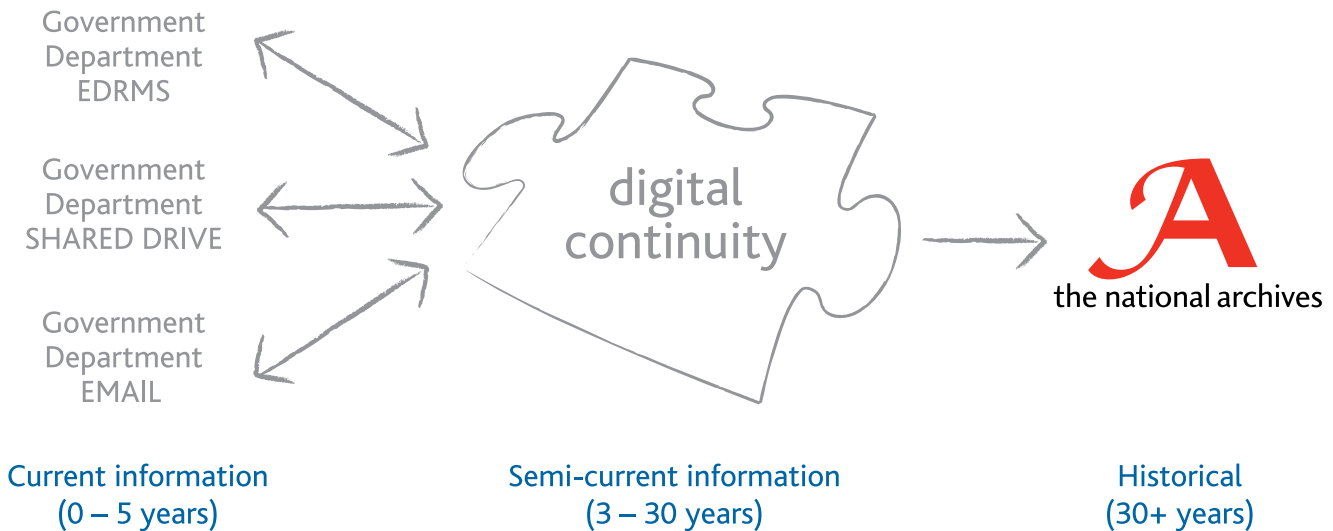
What would happen if vital trial evidence was no longer readable?

digital information **matters**

Did you know?

- An estimated 10 per cent of the Canadian Government's electronic records are already no longer readable.
- A recent study by the National Science Foundation in the US found that the average cost of recreating just 20 MB of data was \$64,000.
- In May 2006, global financial services firm Morgan Stanley agreed to pay \$15 million to settle civil charges by the Securities and Exchange Commission that it failed to produce tens of thousands of emails dating back to December 2000.

Digital continuity – the missing piece



What the digital continuity system will do

- ✓ Determine which format your information is in, generate a plan for ensuring it remains accessible, and action that plan appropriately.
- ✓ Make sure that the information you store is secure from deliberate or accidental damage, such as data corruption, fire or flood.
- ✓ Provide robust content management, including a full audit trail of all actions undertaken.
- ✓ Provide security - up to 'restricted' at the very minimum.
- ✓ Allow you to search across all of your stored data.
- ✓ Work compatibly with your existing systems.
- ✓ Accept data from a wide variety of formats, not just electronic documents and records management (EDRM) systems.

What it won't

- ✗ Provide the forum for you to share information across government; only you have access to the information you store.
- ✗ Take away your responsibility for good information management; digital continuity will only protect the information you choose to save.
- ✗ Replace existing day-to-day filing and content management systems, such as electronic documents and record management (EDRM) systems.
- ✗ Provide a permanent historical archive; although we anticipate the project working compatibly with The National Archives' digital archiving systems.
- ✗ Take away your responsibility for answering Freedom of Information, Data Protection and Environmental Information Regulations.

How it's funded

The project has received funding from across all major departments.

This will enable us to conduct a full assessment of needs; define a product that is technically better and more economical than either departmental options or third party suppliers; and enter into a formal framework agreement, or shared procurement, with a supplier (or suppliers).

Shared procurement brings cost savings as no one department bears the full weight of infrastructure costs. A framework agreement means that you can sign up to the service without having to go through lengthy procurement exercises. The advantage to suppliers is a guaranteed customer base on which to justify investment.

Working with you

We are working with government departments to find out more about how you work, the sort of information you're likely to need access to, and the volumes you're talking about.

This will help us to create a technical specification and a business model.

Your early commitment and support will help us to attract the very best commercial partners.

And if you join us at an early stage you will have a real opportunity to shape product functionality and costs. This is particularly valuable if you have complex requirements.

We are liaising with all government departments to raise awareness of the serious risks of ignoring digital continuity, and to help you plan digital continuity into your future budgets.



Can I access data from the last outbreak of foot and mouth?

digital information **matters**

"Modern government – both in policy making and in service delivery - relies on accurate and timely information about citizens, businesses, animals and assets."

Cabinet Office, Transformational Government
– enabled by technology, 2005

Rest assured

You'll retain complete control over the information you store and who can access it.

You'll still be responsible for all Freedom of Information and Data Protection issues. You'll be able to search for and recall records whenever you need them. Information will be stored safely and will meet stringent security standards.

Working with commercial partners

We're working with external suppliers to develop a digital continuity system, as no suitable product currently exists.

There are products on the market that may store your digital information, but none protect them comprehensively from technological obsolescence. The National Archives has already developed the 'core' of a solution that suppliers could build on - the software and systems of our digital preservation project, *Seamless Flow*. This efficiently archives the digital information that's needed for permanent record and increases public access to it, via The National Archives' website.

The National Archives will act as the central buying authority on behalf of government departments. Once we've agreed a solution and chosen a supplier (or suppliers), our preference is to enter into a formal framework agreement with them. This is where the chosen supplier agrees to a set of conditions and pricing that is valid for all government departments.

"Digital information about nearly every aspect of our lives is being created at an astonishing rate. Locked within all of this data is the key to knowledge about how to cure diseases, create business value, and govern our world more effectively."

Sir Timothy Berners-Lee, founder of the World Wide Web, March 2007



Japanese scandal over lost pensions

A combination of incompatible systems, missing records and wrongly entered details means that around 20 million Japanese people cannot be legally linked with their pension contribution. Those employed before 1997 face an uphill struggle to claim what's rightfully theirs. Confidence in government bureaucracy has been shaken to its core, and experts predict this could lead to an era of exceptional instability for Japanese society.

The Times, 3 July 2007

NASA: scientific data at risk

In 1975, NASA sent two Viking space probes to Mars. The data generated by these unrepeatable missions – produced at a total mission cost of approximately \$1 billion - was recorded onto magnetic tape.

Two decades later, the tapes were cracking and brittle, despite the space agency's best efforts to keep them in a climate-controlled environment. Scientists needed access to the data but were unable to decode the formats used, and none of the original format developers were still alive. In the end, they had to track down old printouts and retype everything. NASA has subsequently become one of the world's biggest supporters of digital continuity projects.

Mind the Gap, Digital Preservation Coalition, 2006

Will we always be able to access information about where nuclear waste is stored?

digital information **matters**

Getting involved

Whether you'd like to get involved at an early stage to shape the solution, or simply find out more, email

digitalcontinuity@nationalarchives.gov.uk
or call Paulette Thompson on **020 8392 5330**
extension **2426**.

If you're an interested supplier, email
digitalcontinuity@nationalarchives.gov.uk
or call Karen Wilson on **020 8392 5330**
extension **2464**.

freedom of information
audits

risk management

compensation

accuracy

responsiveness

parliamentary questions

legal costs

About The National Archives

The National Archives is at the heart of information policy - setting standards and supporting innovation in information and records management across the UK, and providing a practical framework of best practice for opening up and encouraging the re-use of public sector information.

To find out more about the Digital Continuity Project visit
www.nationalarchives.gov.uk/digitalcontinuity

The National Archives

Kew | Richmond | Surrey
TW9 4DU

Published October 2007