



4th Floor, Zone A1
Eland House
Bressenden Place
London SW1E 5DU

7th July 2008

To: All Local Authority Section 151 Officers in England and Wales

Copy: Chief Finance Officer
Chief Information Officers (heads of IT/ICT)
Heads of Housing and Council Tax Benefit Services

Dear Colleague,

Government Connect:

Revised Data Access Policy for DWP RESTRICTED data

This letter is to advise your authority of important developments concerning access to secure case data held on DWP systems. We have also written today to your Leader and Chief Executive outlining the position. To ensure your authority continues to have access to DWP case data beyond 31st March 2009, which is required to support your housing and council tax benefit services, we urge you to:

- a) Take careful note of the revised data access policy described below.
- b) Establish the status of your authority's plans to implement the GCSx¹ secure IT infrastructure being provided by the Government Connect programme.
- c) In the event your authority is unable to implement a live GCSx connection by 31st March 2009 consider making an exemption request to the revised data access policy in accordance with the process described at Annex A.

This letter necessarily includes some terminology you may not be familiar with. Annex B provides explanatory notes to aid your understanding.

Background

You will be aware that on 1st April this year the Permanent Secretaries of DWP, CLG and DCSF along with Paul Coen of the LGA and Janet Callender wrote jointly to Chief Executives of all English and Welsh Local Authorities announcing significant changes to the Government Connect programme. In summary, these changes included:

- a) A £33m funding package to complete the delivery and operation of GCSx to 31st March 2011 with lead responsibility for delivery passing to DWP.
- b) Designation by DWP, CLG and DCSF of GCSx as their preferred method of connection and secure data exchange with English and Welsh local authorities.
- c) A target of 100% English and Welsh local authority connectivity by 31st March 2009.
- d) Confirmation that Government Connect infrastructure (GCSx) would enable the strategic replacement of the interim data encryption solution recently provided by DWP.
- e) Confirmation that from April 2009 the three Departments (DWP, DCSF and CLG) will begin phasing out less efficient, robust or secure internet or postal based methods of communication.

The 1st April 2008 announcement summarised above has enabled a rapid take-up in Government Connect. Fewer than 50 of the 410 English and Welsh local authorities do not have connections or connection requests being processed. The huge potential of secure and trusted IT links with Central Government and other authorities is evidently being recognised as a key enabler to service improvements, greater efficiency and achieving best practise for data protection.

Building on the 1st April announcement, the subsequent significant take-up of Government Connect and the absolute requirement for government departments to protect its RESTRICTEDⁱⁱ information the Government Connect Programme Board is now announcing the first phasing out of less efficient, robust or secure methods of communication.

New DWP Data Access Policy

On 31st March 2009 DWP will cease the provision of RESTRICTED data to local authorities and the receipt of sensitive personal data from local authorities through means other than government approved secure communications channelsⁱⁱⁱ. This policy applies to all authorities in England, Wales and Scotland where a government approved secure communications channel can be or has been made available.

This DWP data access policy means that:

- a) Unless an exemption has been agreed local authority access to the DWP Customer Information Service (CIS)^{iv} over the internet will not be possible after 31st March 2009; in any event internet access to CIS will not be possible after 30th September 2009.
- b) Subject to the availability of the DWP file transfer gateway^v, bulk file transfers between DWP and local authorities currently undertaken as encrypted transmissions over the internet, or by transportation of encrypted physical media, will be replaced with protected communications. To access the DWP file transfer gateway local authorities will require a government approved secure communications channel and a compatible file transfer capability. The technical and commercial implications of this change are being agreed in consultation with local authorities and the LGA and will soon be announced and made available on the Government Connect web site^{vi}.
- c) Local authority access to enhanced business processes^{vii}, which rely on the exchange of DWP RESTRICTED data will depend on communications over a government approved secure channel.

This new DWP data access policy will be incorporated into the Memorandum of Understanding (MoU) between DWP and local authorities, which fully defines the conditions upon which access to DWP data is provided to local authorities. Notwithstanding this new policy ongoing access to DWP data by local authorities is conditional on signature of the latest MoU.

Requests for Exemption

The Government Connect Programme Board will establish an Exemption Committee to consider specific fixed time period requests by local authorities for exemption from the new DWP data access policy. The maximum period of any allowable extension is 6 months commencing 1st April 2009. Further details of the exemption policy and application process are provided at Annex A (attached).

GCSx Code of Connection

The major implication of this new data access policy for local authorities is that continued access to DWP secure data is now dependent on meeting the GCSx Code of Connection^{viii}. The Code of Connection is consistent with well established standards for the management of information security and regarded by government as best practise. For many authorities meeting the Code of Connection will not be a significant undertaking, others will require more work to be done, which is why the exemption process has been established.

DWP is bound by government policy and guidelines for handling RESTRICTED data. GCSx and the associated Code of Connection represent the minimum acceptable level of information security required of local authorities. The data protection act is less explicit and subject to interpretation, but authorities managing sensitive personal data to a lower standard than the GCSx Code of Connection are increasingly at risk of being judged non-compliant^{ix}.

Government Connect will do what it can to help local authorities through the Code of Connection process and to implement GCSx. The programme already provides free consultancy to authorities and has engaged SOCITM to solicit the needs of the local government IT community. With SOCITM we intend to

develop a list of common issues, concerns and needs with a mind to making available services and advice that will help authorities to efficiently implement GCSx.

Progressing the Transformation Agenda

Achieving commonly recognised standards of information security management and trusted communications links across all Government is now more important than ever. Sir Gus O'Donnell sets out in the foreword to the recently released report, "Data Handling Procedures in Government" that, "Effective use of information is absolutely central to the challenges facing government today", and that "Those in public service need to keep that information secure, in order to build public confidence".

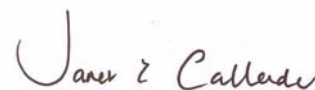
Implementing Government Connect is not only necessary to establish essential controls right now, it also provides a commonly recognised platform upon which all of government can continue to improve its use of data and standards of information security. The Government Connect programme is currently undertaking an exercise to concisely restate the opportunities for local authorities enabled by trusted IT communications. The consultation phase is underway and we would welcome the opportunity to engage with your authority. For more information please contact the Government Connect programme and monitor our website.

Yours sincerely



Joe Harley
Director General, DWP Corporate IT
DWP CIO

Yours sincerely



Janet Callender OBE
Chair - Government Connect Programme Board
Chief Executive Tameside MBC
Chair Local Government Delivery Council

Annex A Requests for Exemption

The Government Connect Programme Board will establish an Exemption Committee to consider specific fixed time period requests by local authorities for exemption from the new data access policy. The Exemption Committee will be chaired by the Government Connect Senior Responsible Owner (SRO) – Kenny Robertson, DWP Director of Transformational Government – and will comprise a subset of the Programme Board, including the LGA, and other specialist advisors. In addition to reporting to the Government Connect Programme Board the Exemption Committee will also report to the DWP Senior Information Risk Owner (SIRO) – Joe Harley, DWP Director General Corporate Information Technology. In the event of dispute the DWP SIRO is the final escalation point and his decision concerning access to DWP data is final.

The Exemption Committee will consider fixed and specific time period requests by local authorities for exemption from the new data access policy subject to the following:

- a) An exemption request is made in writing (by post or e-mail) by the local authority Section 151 officer and received no later than 30th September 2008. Exemption requests should be addressed to the Government Connect Exemption Committee c/o the Government Connect Programme Office, full details can be found on the Government Connect web site.
- b) An exemption request is for a specific, fixed and reasonable period of time not exceeding 6 months commencing 1st April 2009.
- c) The local authority has obtained the GCSx Code of Connection and undertaken an initial review of its GCSx Code of Connection compliance in consultation with their Government Connect Regional Account Manager and submitted an initial draft of their completed Code of Connection to the Government Connect Assessment Team. Please go to the Government Connect web site to obtain details of your Regional Account Manager and to request a copy of the Code of Connection.
- d) The local authority has agreed with the Government Connect Assessment Team areas of current compliance with the Code of Connection and has provided an action plan for compliance with all other mandatory controls the authority is not yet compliant with.
- e) The local authority confirms it has commenced a formally governed project to implement GCSx including a compatible file transfer capability, achieving compliance with the Code of Connection and any other scope items required to achieve operational services over GCSx.
- f) The local authority confirms it will make available to the Exemption Committee reasonable access to details of its project to implement GCSx including specifications, plans, risks, issues, management reports and occasional meetings with key members of the local authority project team.

The Exemption Committee will consider requests for exemption where it is evident that:

- a) The reason for the exemption request is due to specific circumstances that mean it is not reasonable for the local authority to achieve a live GCSx service by 31st March 2009.
- b) The local authority has made implementation of secure communication links an immediate priority and can demonstrate realistic aspirations to implement GCSx as soon as practicably possible.

Annex B Explanatory Notes

ⁱ **GCSx:** GCSx is the Government Connect Secure Extranet. This is the secure network infrastructure being provided to all local authorities in England and Wales through the Government Connect programme. The Departments for Work and Pensions, Children, Schools and Families and Communities and Local Government have collectively fully funded the provision of GCSx to all English and Welsh local authorities through to 31st March 2011.

ⁱⁱ **RESTRICTED information:** While central government processes all personal data in accordance with the Data Protection Act requirements, the act's definitions of "personal" and "sensitive personal data" are not suitable for the administrative definition, or specification of technical protection requirements, for the range of information handled by government. Central government departments therefore operate in accordance with the Manual of Protected Security (MPS). The MPS defines the technical protection requirements for the various categories of information. Information that links an identifiable individual with information that, if released, would put them at significant risk of harm or distress, or alternatively any source of information relating to 1000 or more individuals that is not in the public domain, even if the information is not likely to cause harm or distress, is marked RESTRICTED (though data might also be marked as RESTRICTED for many other purposes). Central government Information Computer and Telephony (ICT) systems handling RESTRICTED information must be accredited to handle such information in accordance with Cabinet Office requirements. Where transfer of RESTRICTED information is necessary this must be over a secure channel.

ⁱⁱⁱ **Government approved secure communications channels:** In the context of this policy announcement Government approved secure communications channels means GSi connections. GSi is the Government Secure intranet, which comprises GCSx, GSX and GSI. The Government Connect programme is delivering GCSx services to all authorities in England and Wales. GSX is similar to GCSx and has already been implemented in all but a few authorities in Scotland. GSI is the service generally used by Central Government and establishes a higher standard of data security than either GCSx or GSX. GSI allows formally accredited (RESTRICTED) networks to connect to one another. GCSx and GSX allow unaccredited networks, such as those typically operated by local authorities, to connect to accredited networks such as those operated by central government and to occasionally receive RESTRICTED data.

^{iv} **DWP Customer Information Service (CIS):** CIS is a DWP managed database that contains personal information on virtually every UK citizen. CIS is likely to become the main source of biographical personal data for the National Identity Scheme and is used by 22,000 people in local authorities to conduct status checks for the purposes of delivering housing and council tax benefit services.

^v **DWP file transfer gateway:** DWP is developing a system called GFTS (Generic File Transfer Service). GFTS will supersede the current mechanism based on the PGP encryption tool used for bulk exchange of benefits data between DWP and local authorities.

^{vi} **Government Connect website:** The Government Connect website is <http://www.govconnect.gov.uk>.

^{vii} **Enhanced business processes:** The DWP Housing Benefits Information Flows Board collectively manages projects, such as E-transfers, HERS and CIS enhancements. The E-transfer project is automating the transfer of DWP data required by local authorities, such as the Local Authority Input Document (LAID) from Job Centre Plus and Local Authority Claim Information (LACI) from the Pensions Service. HERS is a project to improve the bulk exchange of Housing Benefit Matching Service (HBMS) / Single extract data between authorities and DWP. Enhancements are also being made to CIS to include tax credit and ESA related data. Other DWP led projects include In and Out of Work to streamline, through use of electronic forms, the processing of benefits as individuals become in an out of work and Tell Us Once, which emanates from Sir David Varney's work and which aims to provide more citizen centric public services. Initial contact details for all these projects are available through the Government Connect website (<http://www.govconnect.gov.uk>). All of these enhanced business processes are dependent on the transfer of RESTRICTED data and as such will only be available to bodies that have implemented a government approved secure communications channel, such as GCSx.

^{viii} **GCSx Code of Connection:** All GSi connections are subject to the connecting parties' IT services being compliant with the relevant Code of Connection. The GCSx Code of Connection is regarded by government as being equivalent to best practise and the absolute minimum required to handle

RESTRICTED information or personal data, sensitive personal data and protected personal data in the context of the Data Protection Act. The GCSx Code of Connection defines the information security management requirements that must be satisfied by a local authority in order to use its GCSx connection and is based on ISO 27001 (the standard for management of information security).

^{ix} **Data Protection Act compliance:** The recently published report “Data Handling Procedures in Government” establishes a much clearer relationship between data handling in government and the Data Protection Act requirements. Equivalent guidelines for local government are expected to be released by the LGA this summer. Data Protection Act definitions of “sensitive personal data” requiring higher levels of protection – as if protectively marked RESTRICTED – have been clarified with input from the Information Commissioner. The importance of the Data Protection Act has been further underlined with recent changes to include monetary penalties for non-compliance, spot checking powers and even imprisonment for deliberate and reckless abuse.

The seventh principle of the Data Protection Act establishes regard to “...the state of technological development and the cost of implementing any measures...”. This is relevant because government approved secure communication channels are available to all local authorities at no cost to March 2011. A precedent of enforcement has recently been established in relation to the seventh principle. The review by Kieran Poynter of Information Security at HMRC included the following statement, “The Commissioner has informed me that he considers that my Report confirms beyond doubt that HMRC has breached the 7th Data Protection Principle, which requires appropriate technical and organisational measures to be taken against accidental loss of personal data. He has informed me that, accordingly, he proposes as soon as possible to serve an Enforcement Notice on HMRC under section 40 of the Data Protection Act 1998”. Local authorities handling “sensitive personal data” through less secure means than are being provided through Government Connect are at risk of being judged non-compliant and suffering Data Protection Act sanctions in the event of a data loss.