



GCSx – Code of Connection

The Government Connect network is a key enabler in the drive to transform services, with particular focus on joined-up working, shared services, identity management and efficiency gains via solutions that provide secure communication capabilities.

REACT Technologies is an IP security specialist and is currently working with many local authorities to help them resolve their current outstanding security requirements and also provide them with the ability to demonstrate ongoing, monitored and managed compliance in the future.

Our technology portfolio encompasses the Code of Connection requirements. We can work with you on the following areas:

- Incident Response Policy
- Centrally Managed Software Monitoring & Prohibition of Rogue Software
- Improved User Authentication & Controlled Public Access
- Patch Replacement
- Improve Ability to Log, Retain, Store & Analyse Network Activity
- Prohibit Mobile Access From Personal Laptops
- Software Policies
- Improved Control Over Mobile Device Access to GCSx
- Removable Media
- Network Mapping & Schematics
- 12 Monthly Health Check

The GCSx Code of Connection (CoCo) is a list of security controls with which ALL local authorities must be compliant with by **31st March 2009** so GCSx circuits can be activated.

“In the wake of recent data loss incidents and concerns that the public are loosing their trust in governments’ ability to secure personal information, the LGA will be publishing Data Handling Guidelines to help councils meet their responsibilities”

Stephen Jones
(Director of Finance and Performance, LGA)



Make REACT your Technology Partner

We only work with best of breed technologies which are Microsoft recommended or Manual 'Y' Compliant. This key security criteria means the technology in question has been certified for connection to the government's restricted network and has to be met in order for your network to be granted compliancy.

All our solutions are centrally managed and scalable for policy enforcement over multiple site deployments. Whilst still being able to manage, restrict, report and document each individual network port, employee, guest, device, hardware or software activity. Through the integration of these best of breed technologies such as:

- Secure Enterprise Wireless Mobility
- Network Behavioural Analysis
- Infrastructure Mapping
- Infrastructure Monitoring, Trouble Shooting & Incident Management
- Hardware and Software Asset Documentation & Analysis
- End Point Compliance & Network Access Control

Work with REACT to develop your GERSHON Efficiencies strategy, Code of Connection compliance and ensure that your local authority is positioned to secure additional funding in future rounds based on your achievement and success.

If you would like to discuss any of these technologies or your outstanding Code of Connection requirements then please feel free to drop us a line at sales@reacttechnologies.com or call **01256 301900**. Alternatively you can download a FREE trial on a selection of our Infrastructure Management Solutions or arrange a WebEX to overview in more detail.

Main considerations for achieving minimum security requirement

CoCo Challenge Area	Potential Solution
Mobile working arrangements	<ul style="list-style-type: none">• Improve control over mobile device access to GCSx• Restrict data storage on motive devices• Prohibit mobile access from persona: laptops not provided and controlled by local authority• Consider encryption for sensitive data carried on mobile devices• Provision of Dual Factor Authentication
E-mail auto-forwarding	<ul style="list-style-type: none">• Restrict ability to auto-forward GSi family originated emails indiscriminately
Audit logging	<ul style="list-style-type: none">• Improve ability to log, retain, store and analyse network activity
Improving user security	<ul style="list-style-type: none">• Improved system administrator control• Improved user authentication and controlled public access (e.g. via libraries)• Enforcement of more complex passwords
User education	<ul style="list-style-type: none">• Improving understanding of data handing requirements• Introduction of Acceptable Usage Policy and Personal Commit Statements
Software usage	<ul style="list-style-type: none">• Introduction of centrally managed, lower risk software and prohibition of rogue software not controlled from centre
Baseline Personal Security Checking	<ul style="list-style-type: none">• Improved HR polices to enforce personal security checking.• Centralised HR approval' to access GCSx
Removable media availability	<ul style="list-style-type: none">• Improved control over removable media devices such as USB ports and writable disk drives• Incident Response Policy• Document policy covering everything from user helpdesk interactions to management response and escalation procedures