SOUTH CAMBRIDGESHIRE DISTRICT COUNCIL

REPORT TO:	Scrutiny & Overview Committee	3rd September 2009
AUTHOR/S:	Executive Director/ Senior Lawyer	

CALL-IN OF THE GOVERNMENT CONNECT COUNCILLORS EMAIL OPTIONS DECISION BY THE POLICY & PERFORMANCE PORTFOLIO HOLDER ON 21ST AUGUST 2009

BRIEFING NOTE

1. This Note is supplementary to the main report of the Head of ICT supporting the Portfolio Holder Decision of 21st August and its purpose is to explain our statutory obligations regarding the sending of emails. The reasons for the practice changes are fully set out in the main report.

2. The first thing to remember is that data controllers are statutorily liable under the Data Protection Act and therefore have a much higher duty of care than ordinary members of the public when it comes to data processing. The duty is strict and penalties can be imposed against data controllers who flout the law relating to data security. Every day, the Information Commissioner publishes details of offenders who breach data security law. Most high profile breaches are by government departments and public authorities but there are many instances where lawyers, accountants, finance advisors and other professionals have been penalised. In addition, they face potential damages claims from those who suffer loss or embarrassment as a result. Unlawful obtaining or disclosing personal data is a criminal offence triable summarily in the Magistrates Court or on indictment.in the Crown Court.

3. The Council (as a corporate body) is a data controller and therefore any processing of data by officers and members under the corporate umbrella must be done fairly and lawfully (First Principle of the Data Protection Act 1998 – "DPA")). Individual Members will generally be data controllers in their own right also because they process data as part of the constituency or party political activities. Anyone processing data whether under the corporate umbrella of the public authority or as a data controller in their own right must comply with the law or face possible legal action if they do not.

4. Personal data is defined as: "*any information (in manual or electronic form) about a living individual which is capable of identifying that individual. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession"*

5. Sensitive personal data is "*personal data relating to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, alleged or actual criminal activity and criminal record."*

6. Government Connect is about processing personal data and sensitive personal data more securely because it is now accepted that using ordinary email over the internet is not secure and therefore represents a data security risk. Data Controllers who do not take proper measures to keep data secure are more likely to fall foul of the law.

7. Not all emails will contain personal data or sensitive personal data but unfortunately there is no sifting technology available and so responsibility lies with the data controller to ensure that an email containing such information is sent securely or not sent at all. For that

reason, the Council via the Government Connect Code of Connection (CoCo), is no longer allowed to permit the automatic forwarding of email to a lower classification domain such as the internet and/or publicly available Internet Service Providers.

8. Finally, a word or two about the Freedom of Information Act 2000. This is about providing public access (in the name of 'open government') to recorded information held by a public authority or held on behalf of the public authority. Councillors are not public authorities and therefore the regime does not apply to them unless they hold recorded information (in paper form or electronically) on behalf of the Council. Information contained in emails is 'recorded' and therefore disclosable under FOIA unless one or more statutory exemptions applies (e.g. the email contains personal information). This is more likely to affect members of the Executive than non-executive members. The Information Commissioner published a Guidance Note on 4th August 2009 dealing with this subject and it is recommended that all members read it. (www.ico.gov.uk). As with DPA, breaches of FOIA can lead to sanctions and compensation payouts as well as adverse publicity.

Contact Officer: David Lord- Senior Lawyer
Telephone: (01954) 713193