

Council Meeting

9.30am on Tuesday 26th January 2010
Woburn House
Tavistock Square
London
WC1H 9HQ

Ref 08/09-10 **Item 10** **Public agenda**

Report author: David Manning



Members' Responsibilities – Data Protection and Information Assurance

1.0 Purpose of the paper

- 1.1 This paper sets out the revised personal responsibilities of each Council Member for the safeguarding of information they handle in connection with the discharge of their Council responsibilities.
- 1.2 The scope includes: personal and non-personal information in any form, i.e. information on paper or in electronic format.

2.0 Summary

- 2.1 On 6th October 2009 Council considered a set of recommendations from the Executive Committee about Members' data protection and information assurance responsibilities. The principal objection was that the requirement for Members not to use publicly available computers was unachievable. Council did not approve the recommendations and referred the matter back to the Executive Committee to review the requirement and bring revised proposals to the next Council meeting on 26th January 2010.
- 2.2 This paper sets out in Appendix three the original Members' responsibilities, with new text inserted in the light of Member consultation shown in **bold** font within that amended appendix. No text has been removed. These revised responsibilities were approved by the Executive Committee on 12th January 2010.

3.0 Recommendations

- 3.1 Council, upon recommendation of the Executive Committee, are asked to:
 - (1) Discuss and approve the revised Member Data Protection and Information Assurance Responsibilities at Appendix Three;
 - (2) Discuss and approve the Members' Data Protection and Information Assurance Responsibilities Acknowledgement Form at Appendix Four.

4.0 Detail

- 4.1 The GTC has always been committed to observing the principles of the Data Protection Act 1998. In 2008 additional Information Assurance requirements were placed upon the GTC and all public bodies by the Cabinet Office. Information Assurance is the confidence that an organisation has in its arrangements to ensure the confidentiality, integrity and availability of the information it needs to conduct its business.
- 4.2 The GTC, as a public corporation reporting to Parliament, is required to comply with the requirements of the Cabinet Office's Security Policy Framework published in December 2008. It has 70 mandatory requirements. They have to be applied, proportionately, to the management of all information that the GTC, and its contractors, handle. They encompass technical, human and physical aspects of information security. The Security Policy Framework can be viewed online at:
http://www.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf
- 4.3 The GTC reports progress on a range of Information Assurance activities to the Executive Committee and to the Audit Committee on a regular basis, most recently in June 2009. The GTC is required to include a section on Information Assurance in its published Annual Report and Statement on Internal Control to Parliament.
- 4.4 The recent focus of the GTC's Information Assurance efforts has been on staff awareness and training and on reviewing the practices of its contractors. In order to take a comprehensive approach to the management of information risk all aspects of the GTC's information handling need to come within the scope of the GTC's work, including the information handled by or shared with Members (and Additional Committee Members) in connection with their official GTC duties. All Council Members process personal data and confidential non-personal data as part of their role. This includes case papers for regulatory hearings or documents relating to a meeting of a Committee or of the full Council. Currently all of Council's Committees meet in closed session whilst full Council mainly considers public papers although occasionally it considers private papers.
- 4.5 The GTC is legally obliged to take all appropriate technical and organisational measures to avoid unauthorised or unlawful processing of data and to avoid accidental loss or disclosure of the information it holds. Members' awareness and acknowledgement of their responsibilities is a key component of Data Protection and Information Assurance.
- 4.6 The priority is to protect sensitive information, whether that is personal information or non-personal business information. The Members' responsibilities seek to address the risks associated to that when exchanged or accessed electronically. They are general responsibilities, and not specific to any particular computing or communications device.
- 4.7 Since the Council meeting of 6th October 2009 the Information Assurance Manager has spoken to, and corresponded with, two Members about their concerns regarding publicly available computers. In the light of that collaboration, new text and appendices have been developed which: explain the risks in more detail; clarify that the use of computers within a work context is acceptable; and does allow for the use of publicly available computers if individual Members consider it essential in exceptional circumstances. The revised Member Data Protection and Information Assurance Responsibilities were discussed and approved by Executive Committee on 12th January 2010

4.8 This paper and the recommended Data Protection and Information Assurance responsibilities are informed by the advice received from Cabinet Office lawyers, advice from the Departmental Security Unit of the Department for Children, Schools and Families (DCSF), and by the advice of GTC officers.

4.9 When approved by Council, these revised Members' Data Protection and Information Assurance Responsibilities will be uploaded to the Council Members' Extranet and be part of the formal Member Induction programme. All Members will agree to ensure they are familiar with their responsibilities and to complete the Member Data Protection and Information Assurance Responsibilities (Appendix Three), and also the Members' Data Protection and Information Assurance Responsibilities Acknowledgement Form (Appendix Four).

5.0 Previously Defined Member Data Protection and Information Assurance responsibilities

5.1 There is a document on the Members' Extranet which describes the general responsibilities of Members regarding the confidentiality of information they come into contact with in the discharge of the GTC responsibilities, including responsibilities when they cease to be Members. This is the Standing Orders and Corporate Governance Scheme and it includes the Members Code of Conduct (part 5) - Extranet link: <http://i4m.gtce.org.uk/members>. The Member Corporate Induction reinforces these points. In addition, Members were reminded of their responsibilities for the safe-keeping of case papers in the Members Regulatory Bulletin: August 2009 in section 3, "Information Assurance: Security of Case Papers and related matters".

5.2 This paper builds upon the guidance in those documents, and provides greater detail compatible with the specific requirements of the Cabinet Office's Security Policy Framework.

6.0 Financial and procurement implications

6.1 There are a wide range of financial implications arising from the GTC's commitment to Data Protection and Information Assurance. No direct financial implications have been identified in relation to this paper and its recommendations.

7.0 Risk management implications

7.1 The adoption of and adherence to a clear statement of Members' Data Protection and Information Assurance responsibilities will contribute to the GTC's management of information risk.

8.0 Equality and diversity implications

8.1 There are none.

Appendices

Appendix One: Cabinet Office guidance

Appendix Two: Risks to GTC Members' privacy and confidentiality arising from using publicly available computers

Appendix Three: Member Responsibilities – Data Protection and Information Assurance

Appendix Four: Data Protection & Information Assurance Responsibilities – Member Acknowledgement Form

Appendix Five: Glossary

Person responsible for the paper:

Name Sally Staples Director of Corporate Services (Senior Information Risk Owner)
Tel: 0121 345 0020 Email: sally.staples@gtce.org.uk

Author:

David Manning, Information Assurance Manager
Tel: 0124 345 0053 Email: david.manning@gtce.org.uk

Lead Member:

Barbara Hibbert, Lead Member for Communications

Date of sign off of paper: 14th January 2010

Cabinet Office Guidance

Cabinet Office guidance about remote working is too extensive and detailed to quote in full.

The particular guidance relating to accessing information from computer equipment that does not sit within the organisation's network (i.e. is not belonging to the GTC) is contained within the HMG Information Assurance Standard No.6 – Protecting Personal Information and Managing Risk. This standard states the requirements of those originally placed on the GTC in July 2008, which were previously known as the “Hannigan Requirements”.

The standard approves the use of internet cafes only for general use of the internet such as using the BBC News website and searching for public domain information via Google.

Where user names and passwords are required to access information systems then internet cafes are not an approved means of accessing them. This applies to accessing email accounts that require input of a user name and a password, and accessing the Members' extranet which contains private papers and potentially sensitive business information.

Risks to GTC Members' privacy and confidentiality arising from using publicly available computers

Essential information

Computers that are available for public use, especially those in Internet Cafes, can often appear to be a convenient place to do work but expose users to considerable risks. As the computer can be used by anyone its security is not under the user's control and it may have *SPYWARE* installed for malicious purposes.

SPYWARE can record keystrokes typed on a keyboard and take screenshots (pictures of the information displayed on the monitor) at regular intervals. The *SPYWARE* can record the business or private information being viewed, logon details to Internet banking profiles, e-mail account profiles, Facebook profiles, etc. Therefore, business including GTC information is put at potential risk, as well as anything a Member does with respect to their wider professional and private life.

The *SPYWARE* forwards the recorded details to the attacker. Using this information, the attacker is able to log into the compromised accounts. The attacker could then use this information to steal a person's identity or use the information for other criminal intent.

Further reading

More information about the risks associated with using publicly available computers the following websites articles are recommended:

- 1. Use public computers carefully** – an article on the government's Get Safe On Line website at http://www.getsafeonline.org/nqcontent.cfm?a_id=1131
- 2. What security software should be installed on Internet cafe computers?** An article by Michael Cobb 6 April 2009 available at: <http://www.searchsecurityasia.com/content/what-security-software-should-be-installed-internet-cafe-computers>

Members' Responsibilities Data Protection and Information Assurance

1. Channels of communication between Members and GTC staff

- 1.1 The GTC has established ways of exchanging regulatory case papers with Members securely. Members detailed responsibilities for the safe-keeping of case papers are documented in the Members Regulatory Bulletin: August 2009 in section 3," Information Assurance: Security of Case Papers and related matters".
- 1.2 For non-regulatory work, the recommended means of exchanging written information are:
 - a. Email.
 - b. Documents attached to emails, with the documents password protected if they contain sensitive information, and the password provided separately by another channel of communication.
 - c. The Members Extranet.
 - d. Physical papers in the post. The papers should be securely sealed in sufficiently robust envelopes appropriate to the nature and amount of paper being sent and with the correct postage paid.

2 Physical security of GTC information in electronic form

- 2.1 To protect the GTC from avoidable reputational damage GTC information that is not in the public domain should not be transferred onto any electronic portable storage devices such as USB memory sticks, CDs, DVDs.
- 2.2 If a Member uses a laptop, BlackBerry, **iPhone** or any other mobile **communications** device they should keep it with them when they are travelling and ensure the information on it is not read in circumstances where it may be visible to others.
- 2.3 Members should only retain GTC emails and save and retain electronic GTC documents where it is appropriate and for as long as is necessary. Emails or attachments, or downloaded documents from the Members' Extranet should only be kept for so long as is necessary. Emails and documents that are no longer required should be deleted from the Inbox, Deleted Email folder and the Recycle Bin as appropriate. On no account should Members save sensitive personal information provided by the GTC to their personal or work related computer.

3 Physical security of GTC information on paper

To ensure the physical security of GTC information on papers Members should do the following:

- 3.1 Ensure the GTC has their up-to-date postal address to ensure safe transfer of information to them.
- 3.2 Keep papers safe and restrict access to them whether at home or at work.

- 3.3 Ensure papers are kept in their possession at all times when travelling and are not read in circumstances where their content may be visible to others.
- 3.4 Store personal or confidential non-personal information securely when not in use. For example, papers should not be left unattended in a car.
- 3.5 Dispose of papers by either shredding them or by using an accredited confidential waste service. GTC confidential papers should not be put into general household waste or sent for recycling (unless they have been shredded first). At Committee and Council meetings Members may return papers to the Council Secretariat.

4. Accessing GTC information over the Members' Extranet and by email

- 5.1 Members must ensure the GTC has their up-to-date email contact details to ensure safe transfer of information to them.
- 5.2 Members should only use computers on which antivirus software and operating system updates are kept up-to-date. **Unless an individual Member decides that it is essential, Members should not use publicly available computers (e.g. at an internet café, hotel or library) to access emails with the GTC or to use the GTC's Extranet, and then only to access non-sensitive information. This requirement applies regardless of what type of computer it is – i.e. Windows based PC or laptop, or an Apple Mac. Using publicly available computers presents a real risk to Members' own business and personal information.**
- 5.3 **It is acceptable for Members to use the computers they use at their place of employment, for example at school, providing those are protected with appropriate anti-virus software.**
- 5.4 Members are responsible for ensuring only authorised people can access their emails with the GTC and that those people clearly understand their responsibilities for ensuring the confidentiality of the information that those emails contain.
- 5.5 Members should ensure passwords are kept private, are not shared and are kept secure.

5.0 Action Members should take if they think confidential GTC information has been lost or has been accessed by unauthorised people.

- 5.1 If Members become aware of a loss of information or if they believe that GTC information has been accessed by any unauthorised third parties they should in the first instance contact the Council Secretary. If the Council Secretary is unavailable, or if the incident occurs outside normal office hours, Members should contact the GTC's Senior Information Risk Owners (SIROs).
- 5.2 The contact details for the Council Secretary and the SIROs follow.

Mike Herlihy
mike.herlihy@gtce.org.uk
Office: 020 7023 3914
Mobile: 07884 235785

Sally Staples
sally.staples@gtce.org.uk
Office: 0121 345 0020
Mobile: 07789652146

Alan Meyrick
alan.meyrick@gtce.org.uk
Office: 0121 345 0050
Mobile: 07879434492

6.0 Advice to Members on Data Protection and Information Assurance

- 6.1 If a Member has any query relating to the processing of personal data or other confidential information in their role as a Council Member they should contact a member of the GTC's Information Assurance Team, or the Data Protection Officer, at the first opportunity. Their contact details follow:

David Manning, Information Assurance Manager
david.manning@gtce.org.uk 0121 345 0053

John Thompson, Information Assurance Officer
john.thompson@gtce.org.uk 0121 345 0014

Noreen Doyle, Information Security Officer
noreen.dolye@gtce.org.uk 0121 345 0153

Stephen Goldsby, Data Protection Officer
stephen.goldsby@gtce.org.uk 0121 345 0137

- 6.2 An excellent non-technical introduction to practical things people can do to protect confidential information is available on the government website called "Get Safe Online". The website address is: <http://www.getsafeonline.org/>

Members' Responsibilities

Data Protection & Information Assurance Member Acknowledgement Form

Terms of Reference

Within the context of this confidentiality statement, the term "GTC data" shall be taken to mean personal data and any confidential non-personal information held by the GTC.

Processing of GTC Data (accessing, disclosing or destroying data)

GTC data must only be processed to fulfil the purposes specified in the GTC's notification under the Data Protection Act 1998. These purposes may be viewed on the Register of Data Controllers at www.ico.gov.uk

Under the terms of the Data Protection Act 1998 and the Computer Misuse Act 1990, unauthorised processing of GTC data may result in both the GTC and the individual concerned being subject to legal proceedings.

Accessing GTC Data

You must only access GTC data if you have been properly authorised to do so and access is necessary for you to carry out your work for the GTC. Unauthorised accessing of GTC data may result in action under the Members Code of Conduct.

Disclosure of GTC Data

Unless you are authorised to do so as part of your GTC responsibilities, you must not disclose, divulge, or transfer GTC data by any means whatsoever to any persons either within or beyond the GTC. After the termination of your duties for the GTC, you must not disclose, divulge, or transfer any GTC data, acquired by reason of those duties, by any means whatsoever to any persons either within or beyond the GTC.

Destruction of GTC data

Unless you are required to do so in the proper course of your duties for the GTC, you must not conceal, erase or destroy any GTC data.

Tick boxes as appropriate.

- I have read and understood the above statement and have had an opportunity to discuss it with the Council Secretary.
- I have read, understood and will adhere to the current Members' Data Protection and Information Assurance Responsibilities located on the Members Extranet.
- If at any future date I have a doubt as to whether I may access, disclose, or destroy GTC data, I will ask the Council Secretary, the Data Protection Officer or the Information Assurance Manager.

Name: (please print)

Signature:

Date:

Glossary

1. Antivirus software
Software that is used to prevent, detect, and remove malicious computer programs, including computer viruses and spyware.
2. Security Policy Framework
The Cabinet Office document published December 2008 that sets out the universal mandatory standard for the secure handling of personal and non-personal sensitive information, as well as providing guidance on risk management and defining new compliance and assurance arrangements. It applies to all central government departments and related bodies, such as the GTC.
3. Spyware
Unwanted software that secretly monitors a user's activity, scans for private information or gives outsiders control of a computer