

Report to: **Governance Committee**
Date: **4 September 2009**
By: **Deputy Chief Executive & Director of Corporate Resources**
Title of report: **Implementation of a Government Connect Secure Extranet Acceptable Usage Policy and Personal Commitment Statement.**
Purpose of report: **Proposal for the introduction of a Government Connect Secure Extranet Acceptable Usage Policy and Personal Commitment Statement.**

RECOMMENDATIONS

The Governance Committee is recommended to approve the introduction of a government Connect Secure Extranet Acceptable Usage Policy and Personal Commitment Statement.

1. Financial Appraisal

1.1 There are no increased costs arising from the recommendations in this report but ensuring compliance with the whole Government Connect requirements so far cost some £140,000.

2. Supporting Information

Introduction

2.1 The Government Connect Secure Extranet (GCSx) is a secure private Wide-Area Network (WAN) which enables secure interactions between connected Local Authorities and organisations.

2.2 In order to be able to be granted a connection to GCSx, East Sussex County Council (ESCC) is required to submit a completed Code of Connection (CoCo) and to be adjudged by Government Connect as being compliant.

2.3 A number of criteria have to be satisfied in order to be judged compliant and these represent best practice with regard to measures which ensure protection of restricted information. One of these is the implementation of an Acceptable Usage Policy and Personal Commitment Statement which will apply to those ESCC personnel who require access to the GCSx.

Benefits of Connectivity

2.4 This is an exercise that is being undertaken by all local authorities in England and Wales. For those authorities that operate Revenue and Benefits functions, compliance was required by 31 March 2009 in order to continue to exchange information with the Department for Work and Pensions. For ESCC it is anticipated that connectivity will be required for our involvement in a number of Government initiatives including:

- Implementation of the European Services Directive in the UK
- Putting People First
- DSCF initiatives such as Contact Point, Common Assessment Framework, Key to Success (Access to School Performance Data) and Free School Meals (eligibility checking)
- Justice initiatives such as Youth Offending (data sharing between Youth Justice Board and Youth Offending Teams) and Asset Recovery (SOCA) (improved data access)

2.5 The benefits are arguable, but effectively the Council has to comply.

Visibility for Members

2.6 Government Connect has not detailed any scenarios which would involve members requiring access to the GCSx. However, Members will be affected by the general changes required to make the Council's ICT infrastructure sufficiently secure to enable it to be connected to the GCSx. The major visibility will be in the following areas:

Passwords: These will need to be "complex" - a combination of upper case letters, lower case letters, numbers and symbols and at least 9 characters in length.

Encryption of portable media (e.g. laptops, USB memory sticks, PDAs smartphones): This is covered by the Council's Data in Transit Policy. This will require laptop users to log in twice; first to log on to the laptop and second to log on to the network (the same user-id/password will be used for both).

Dual Factor Authentication: Personnel who access the Council's network remotely using an ESCC laptop will need to use dual factor authentication - in addition to signing on with a user-id/password, a token will be required.

Timescales

2.7 For East Sussex County Council, the deadline for compliance is 30th September 2009.

2.8 The schedule that has to be adhered to in order to ensure the acceptance of the Acceptable Usage Policy and Personal Commitment Statement in line with the deadline for compliance is:

8th July 2009: Trade Union Business Meeting (no issues raised)

22nd July 2009: Chief Officers Management Team Meeting (approved)

4th September 2009: Governance Committee Meeting

3. Conclusion and Reason for Recommendation

3.1 In order to be granted connectivity to the Government Connect Secure Extranet by the Government's deadline of 30 September 2009, and to be able to participate fully in future Government programmes, it is recommended that the Governance Committee approves the implementation of the Acceptable Usage Policy and Personal Commitment Statement referenced in this document.

SEAN NOLAN
Deputy Chief Executive and
Director of Corporate Resources

Contact Officer: Eric Hanslip Tel No. 01273 482099

Local Members: All

Background docs: None

Policy Document

Government Connect Secure Extranet Acceptable Usage Policy and Personal Commitment Statement

Contents

1	Definition	2
2	Policy Statement	2
3	Purpose	2
4	Who does this policy apply to?	3
5	Risks	3
6	GCSx Acceptable Usage Policy	3
7	Policy Compliance	6
8	Policy Governance.	6
9	Review and Revision	6
10	GCSx Personal Commitment Statement	6

1 Definition

1.1 The Government Connect Secure Extranet (GCSx) is a secure private Wide-Area Network (WAN) which enables secure interactions between connected Local Authorities and organisations that sit on the pan-government secure network infrastructure.

2 Policy Statement

2.1 It is East Sussex County Council policy that all users of GCSx understand and comply with corporate commitments and information security measures associated with GCSx.

2.2 It is anticipated that connectivity to the GCSx will be an increasing requirement from the Government with respect to ensuring that communications and transfer of data between the County Council and Central Government departments and other agencies.

2.3 The following East Sussex County Council policy documents are directly or indirectly relevant to this policy:

2.3.1 Email Use Policy:

<http://intranet.escc.gov.uk/personnel/working/payconditions/pages/esccemailsystem.aspx>

2.3.2 Internet Access and Usage Policy:

<http://intranet.escc.gov.uk/personnel/Documents/az/internetaccess.doc>

2.3.3 Data in Transit Policy:

http://intranet.escc.gov.uk/helping/dataandrecords/security/Documents/data_in_transit.doc

2.3.4 Information Security Policy:

http://intranet.escc.gov.uk/helping/ict/Documents/information_security_policy.rtf

2.3.5 (Adult Social Care and Children's Services) Mobile Teleworking Policy

http://escctrinet/home/socserv/guidance_and_info/security/ig%20docs/information%20security/314endorsedmobileteleworkingpolicyfrontpage.doc

3 Purpose

3.1 The purpose of this Policy is to ensure that the Council is complying with the requirements as laid down by Government Connect for local authorities when access is granted to the GCSx.

3.2 Some Council staff will be required to have access to the facilities operated on the GCSx in order for them to carry out their business. This may include staff having access to a secure email facility. All staff requiring access to the GCSx network in any way will be required to read and understand this Acceptable Usage Policy (AUP) and sign the Personal Commitment Statement.

3.3 This policy and statement does not replace the Council's existing Email Use, Internet Access and Usage, Data in Transit, Information Security or any other, policies; it is a supplement to them.

4 Who does this policy apply to?

4.1 All users of the GCSx connection must be aware of the commitments and security measures surrounding the use of this network. This policy must be adhered to by all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council using the GCSx facilities.

4.2 This policy must be adhered to at all times when accessing GCSx facilities

5 Risks

5.1 East Sussex County Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

5.2 By requiring personnel to be aware of the operational requirements detailed in this policy, the policy aims to mitigate risks including the following:

5.2.1 Access to GCSx by unauthorised personnel

5.2.2 Access to GCSx from unauthorised equipment or locations

5.2.3 Unauthorised transfer of sensitive information

5.2.4 Insecure storage of information including transport of computer media and portable computers

5.2.5 Inadequate destruction of data

5.2.6 The non-reporting of information security incidents

5.2.7 The loss of direct control of user access to information systems and facilities

5.2.8 Introduction of viruses, Trojan horses or other malware

5.2.9 Failure to comply with the Data Protection Act 1998 and any other relevant legal, statutory or contractual obligations

5.3 Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

6 GCSx Acceptable Usage Policy

6.1 Each GCSx user must:

6.1.1 read, understand and sign to verify they have read and accepted this policy;

6.1.2 understand and agree to comply with the security rules of the County Council.

6.2 For the avoidance of doubt, the security rules relating to secure e-mail and information systems usage include:

- a) I acknowledge that my use of the GCSx may be monitored and/or recorded for lawful purposes.
- b) I agree to be responsible for any use by me of the GCSx using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address; and,
- c) I will not use a colleague's credentials to access the GCSx and will equally ensure that my credentials are not shared and are protected against misuse; and,
- d) I will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises); and,
- e) I will not attempt to access any computer system that I have not been given explicit permission to access; and,
- f) I will not attempt to access the GCSx other than from ICT equipment and systems and locations which have been explicitly authorised to use for this purpose; and,
- g) I will not transmit information via the GCSx that I know, suspect or have been advised is of a higher level of sensitivity than my GCSx domain is designed to carry; and,
- h) I will not transmit information via the GCSx that I know or suspect to be unacceptable within the context and purpose for which it is being communicated; and,
- i) I will not make false claims or denials relating to my use of the GCSx (e.g. falsely denying that an e-mail had been sent or received); and,
- j) I will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the GCSx to the same level as I would paper copies of similar material in line with appropriate legislation and East Sussex County Council policies and standards; and,
- k) I will appropriately label (e.g. within document titles, footers, filenames), using the HMG Security Policy Framework (SPF) (see Appendix A for details), information up to RESTRICTED sent via the GCSx; and,
- l) I will not send PROTECT or RESTRICTED information over public networks such as the Internet unless it is necessary to transfer personal information to organisations without GCSx connectivity, in which case this will be achieved by using secure e-mail or encryption and in compliance with Data Protection legislation; and,

- m) I will always check that the recipients of e-mail messages are correct so that potentially sensitive or PROTECT or RESTRICTED information is not accidentally released into the public domain; and,
- n) I will not auto-forward email from my GCSx account to any other non-GCSx email account; and,
- o) I will not forward or disclose any sensitive or PROTECT or RESTRICTED material received via the GCSx unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel; and,
- p) I will seek to prevent inadvertent disclosure of sensitive or PROTECT or RESTRICTED information by avoiding being overlooked when working, by taking care when printing information received via GCSx (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc) and by carefully checking the distribution list for any material to be transmitted; and,
- q) I will securely store or destroy any printed material; and,
- r) I will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via GCSx and,
- s) where ICT Services have implemented other measures to protect unauthorised viewing of information displayed on ICT systems (such as an inactivity timeout that causes the screen to be blanked requiring a user logon for reactivation), then I will not attempt to disable such protection; and,
- t) I will make myself familiar with the Council's security policies, procedures and any special instructions that relate to GCSx; and,
- u) I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security; and,
- v) I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended; and,
- w) I will not remove equipment or information from council premises without appropriate approval; and,
- x) I will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist theft) in accordance with the Council's Data in Transit Policy; and,
- y) I will not introduce viruses, Trojan horses or other malware into the system or GCSx; and,
- z) I will not disable anti-virus protection provided at my computer; and,

- aa) I will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that the Council informs me are relevant; and,
- bb) if I am about to leave the Council, I will inform my manager prior to departure of any important information held in my account and manage my account in accordance with the Council's Information Security Policy.

7 Policy Compliance

- 7.1 If any user is found to have breached this policy, they may be subject to East Sussex County Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).
- 7.2 If you do not understand the implications of this policy or how it may apply to you, seek advice from your E-Business Manager.

8 Policy Governance.

- 8.1 The Deputy Chief Executive/Director of Corporate Resources has ultimate responsibility for the policy but on a day to day basis the Head of ICT is responsible for developing and implementing the policy.
- 8.2 The following were consulted prior to final policy implementation:
 - 8.2.1 PAT HR Strategy Group (8th June 2009)
 - 8.2.2 ICT Senior Managers
 - 8.2.3 E-Business Managers
 - 8.2.4 Trades Unions (Trades Union Business Meeting 8th July 2009)
 - 8.2.5 Chief Officers Management Team (22nd July 2009)

9 Review and Revision

- 9.1 This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.
- 9.2 The policy review will be undertaken by Head of ICT.

10 GCSx Personal Commitment Statement

I, _____ *[insert user's name]*, accept that I have been granted the access rights to GCSx. I understand and accept the rights which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access services or assets that I am not authorised to access, may lead to disciplinary action and specific sanctions. I also accept and will abide by this policy, personal commitment statement, email use, internet access and usage, data in transit and information security policies. I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of the Council's disciplinary policy.

Signature of User: _____

Date: _____

A copy of this agreement is to be retained by the User and E-Business Manager.

DRAFT

Appendix A: HMG Security Policy Framework Definitions of PROTECT and RESTRICTED

Criteria for assessing RESTRICTED assets:

- affect diplomatic relations adversely;
- cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness or security of United Kingdom or allied forces;
- cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or companies;
- prejudice the investigation or facilitate the commission of crime;
- breach proper undertakings to maintain the confidence of information provided by third parties;
- impede the effective development or operation of government policies;
- to breach statutory restrictions on disclosure of information;
- disadvantage government in commercial or policy negotiations with others;
- undermine the proper management of the public sector and its operations.

Criteria for assessing PROTECT (Sub-national security marking) assets:

- cause distress to individuals;
 - breach proper undertakings to maintain the confidence of information provided by third parties;
 - breach statutory restrictions on the disclosure of information;
 - cause financial loss or loss of earning potential, or to facilitate improper gain;
 - unfair advantage for individuals or companies;
 - prejudice the investigation or facilitate the commission of crime;
 - disadvantage government in commercial or policy negotiations with others.
-

For use by ICT Services only:

Name of User:	
Position:	
Department:	
User Access Request Approved by:	E-Business Manager Name: Position: Date:
User Access Request Approved by:	Name: Date:
Username Allocated	
Email Address Allocated:	
User Access Request Processed:	Name: Date: