Cheltenham Borough Council
Cabinet – 17 March 2015
O&S Committee 2 March 2015
Information Security Policy

Accountable member	**Cabinet Member Corporate Services, Councillor Jon Walklett**
Accountable officer	**Director of Corporate Resources, Mark Sheldon**
Ward(s) affected	**None**
Key Decision	**No**
Executive summary	As part of the council's connection to the Public Services Network (PSN) it is required to have in place an Information Security Policy. . Since the creation of ICT Shared Services with Forest of Dean District Council (FoDDC) we have been developing a Joint Information Security Policy for all the partners in the ICT Shared Service. This has now been completed and agreed by the Joint Security Working Group, adopted by the FoDDC Cabinet and is now recommended to Cheltenham Borough Council's Cabinet for adoption. This policy will provide guidance to all ICT users and help to keep our systems and data secure.
Recommendations	**That Cabinet consider the attached Information Security Policy and adopt it for the use by all CBC ICT users**

Financial implications	There are no financial implications arising from this report **Contact officer: Mark Sheldon** **Email; mark.sheldon @cheltenham.gov.uk,** **Tel; 01242 264123**

Legal implications	The legal implication of not having a robust IT security policy could be failure to comply with the Data Protection Act 1998 and the PSN requirements. Loss of personal data could result in a financial penalty from the Information Commissioner and/or loss of the PSN connection resulting in the council being unable to provide benefits and meet it statutory requirements. **Contact officer: Sarah Halliwell** ***sarah.halliwell@tewkesbury.gov.uk,*** ***Tel; 01684 272692***
HR implications (including learning and organisational development)	The HR implications are as outlined in this report. **Contact officer: Carmel Togher** ***carmel.togher @cheltenham.gov.uk, 01242 775215***
Key risks	Failure to have an adequate Information Security Policy in place and to enforce that policy could result in the council's PSN (Public Services Network) connection being terminated.
Corporate and community plan Implications	Supports the Corporate Strategy outcome of - Transform our council so it can continue to deliver our outcomes for Cheltenham and its residents
Environmental and climate change implications	None
Property/Asset Implications	None Contact officer: @cheltenham.gov.uk

Background

1.1 Information security is concerned with ensuring that we keep information confidential, accurate and available to those who need it. We store information in many formats such as emails, letters and CCTV footage.

1.2 When dealing with confidential data, both personal and commercial, we follow current legislation such as:

- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations

1.3 ICTSS has developed this to take on the needs of all of its ICT users in terms of information security and covers both paper and electronic information.

1.4 This policy applies to all staff and Members. It is the responsibility of all staff and Members to ensure they read and understand their obligations under it.

1.5 In meeting its Information Security responsibilities ICTSS and therefore Cheltenham Borough Council adopts the four key principles described by HM government:

> **Principle 1**: **ALL information** that HMG needs to collect, store, process, generate or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection.
>
> **Principle 2**: **EVERYONE** who works with government (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training.
>
> **Principle 3:** Access to sensitive information must **ONLY** be granted on the basis of a genuine „need to know and an appropriate personnel security control.
>
> **Principle 4:** Assets received from or exchanged with external partners **MUST** be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

1.6 This policy should be read in conjunction with the Acceptable Usage Policy and Personal Commitment Statement, and the Internet Acceptable Usage Policy signed by all staff. These documents are available to all employees and elected members through the ICTSS web page on the intranet.

2. Reasons for recommendations

2.1 The council has a responsibility to ensure that all of its information and data is collected, used, stored and transmitted in secure and effective manner; this policy will support that overall objective.

3. Alternative options considered

3.1 None

4. Consultation and feedback

4.1 Officers from FoDDC and Cheltenham Borough Council who make up the Joint Security Working Group considered the Information Security Policy and recommended it for approval and use.

5. Performance management – monitoring and review

5.1 ICTSS have delegated responsibility for the management of CBC ICT systems and Information Security and they will apply and enforce the policy in that respect. Responsibility for the management of paper records and local security for Cheltenham Borough Council will be monitored by the Security Working Group and the Information Management Group, assurance on compliance will be provided by Directors on an annual basis.

Report author	**Contact officer: Corporate Governance, Risk and Compliance officer** **Email; Bryan.Parsons@cheltenham.gov.uk,** **Tel; 01242 264189**

Appendices	1. Risk Assessment 2. Information Security Policy
Background information	FoDDC Cabinet minute for ICT Information Security Policy

Risk Assessment

Appendix 1

The risk				Original risk score (impact x likelihood)			Managing risk				
Risk ref.	Risk description	Risk Owner	Date raised	Impact 1-5	Likeli-hood 1-6	Score	Control	Action	Deadline	Responsible officer	Transferred to risk register
	If the Council fails to approve an adequate Information Security Policy, and to enforce it then it could result in the council's PSN (Public Services Network) connection being terminated.	Director Corporate Resources	17/03/2015	3	2	6	reduce	Request that Cabinet adopt the ICTSS Information Security Policy for CBC ICT users	17/03/2015	Corporate Governance, Risk and Compliance officer	
	If the Council fails to approve an adequate Information Security Policy, and to enforce it then it could result in the Council's information being put at risk	Director Corporate Resources	17/03/2015	3	2	6	reduce	Request that Cabinet adopt the ICTSS Information Security Policy for CBC ICT users	17/03/2015	Corporate Governance, Risk and Compliance officer	

Explanatory notes

Impact – an assessment of the impact if the risk occurs on a scale of 1-5 (1 being least impact and 5 being major or critical)

Likelihood – how likely is it that the risk will occur on a scale of 1-6

(1 being almost impossible, 2 is very low, 3 is low, 4 significant, 5 high and 6 a very high probability)

Control - Either: Reduce / Accept / Transfer to 3rd party / Close