Report of	Meeting	Date
Corporate Director (ICT) (Introduced by the Executive Member for Resources)	Executive Cabinet	8th January 2009

NEW INFORMATION SECURITY FRAMEWORK

PURPOSE OF REPORT

1. To gain approval of the new Information Security Framework and the implementation of the measures contained therein.

RECOMMENDATION(S)

2. It is recommended that Executive Cabinet approve the Information Security Framework to replace the existing IT Security Policy.

REASONS FOR RECOMMENDATION(S)

(If the recommendations are accepted)

3. The existing IT Security Policy requires updating and does not effectively deal with the threats facing the Council. The new framework is designed to move the Council towards the recognised international security standard ISO 27001.

ALTERNATIVE OPTIONS CONSIDERED AND REJECTED

4. Minor amendments to the existing policy.

CORPORATE PRIORITIES

5. This report relates to the following Strategic Objectives:

Put Chorley at the heart of regional economic development in the Central Lancashire sub-region		Develop local solutions to climate change.	
Improving equality of opportunity and life chances		Develop the Character and feel of Chorley as a good place to live	
Involving people in their communities		Ensure Chorley Borough Council is a performing organization	X

BACKGROUND

6. The Council is entirely dependent upon it's information and information systems to deliver services. More importantly it is dependent upon these critical resources to meet statutory obligations. It is important that we put in place the policies and procedures necessary to protect both the information in our custody and, as a consequence, those who trust us with it.

7. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The three

primary tenets of information security are confidentiality, integrity and availability or, as they are often referred to, 'CIA'.

- **Confidentiality** - Ensuring that only authenticated authorised entities have appropriate access to information. Encryption is the most commonly used tool to achieve confidentiality.
- **Integrity** - We need to ensure that our information systems, and the information contained within them, are protected from modification by unauthorised parties as well as improper modification by authorised ones.
- **Availability** - Information systems serve no purpose if they, and the information they contain, are not readily accessible to authenticated, authorised users and systems with appropriate levels of access rights as and when needed.

Our security policies must put in place the provisions to ensure we can address the requirements of these principles as far as is practical.

8. It is also important to note the clear links between good information security and our obligations under legislation. Compliance with the eight principles of the Data Protection Act is clearly dependent upon good information security as is meeting our responsibilities under the Freedom of Information Act.

9. Members will be aware of the recent high-profile incidents relating to the loss of personal information by public sector organisations such as HMRC. As a result of recent high profile information security incidents, partners such as the DWP will require evidence of our commitment to secure the information they provide to us. Recent developments mean that, unless we can demonstrate we have, in place, a security policy which is fit for purpose, the DWP will halt their data exchange with us.

10. In operational terms, we must ensure that the information upon which we base decisions is accurate and current and we must be able to demonstrate to others that working with us will not compromise their information security.

11. The Council is committed to meeting these obligations and, as a result, initiated a review of the current IT Security Policy using the international standard ISO 27001 as a guide. The existing policy served a purpose but does not reflect the changes in working practices that have taken place in recent years as well as those we expect in the future, such as mobile and home working. These changing work practices expose the Council's information and information systems to a myriad of new threats. Our Information Security policies must recognise these threats and mitigate the risks that result.

THE FRAMEWORK

12. The many aspects of information security mean that our Framework is not a short document. However, we should remember that our security policies and systems are only as strong as their weakest link therefore the document must cover all of the main characteristics of a secure environment. In recognition of this, the framework has been segmented into sections which focus upon particular areas e.g. user guidelines, password security etc. This, together with the colour coding, will allow staff to focus on areas which affect them and be able to quickly reference other policies should they become relevant.

13. New staff will be required to read the whole document and signify their understanding and acceptance prior to gaining access to the Council's ICT systems. Existing staff will be required to provide the same documentary assurance or face having their network access revoked.

14. Members will understand that the threats we face will continually develop and, as a result, we must continually review this document. We must be quick to react to security incidents

or near misses to prevent reoccurrence. As a result, following the first issue of the framework, staff will be instructed that the current version will reside on the Loop and they will be notified of updates.

15. Members will see that as part of the policy, we are to define incident reporting procedures (that will include references to the Whistle blowing Policy) to ensure they are consistent and easy to follow. The procedures are in the final phase of development and will be in place by the end of January.

16. The framework document can be located on the Loop at http://theloop/section.asp?catid=12172&docid=19845

IMPLICATIONS OF REPORT

17. This report has implications in the following areas and the relevant Corporate Directors' comments are included:

Finance		Customer Services	
Human Resources	X	Equality and Diversity	
Legal	X	No significant implications in this area	

COMMENTS OF THE ASSISTANT CHIEF EXECUTIVE (TRANSFORMATION)

18. The security of the Council's assets is clearly a key concern. This framework requires the implementation of best practice in a number of areas and will reduce the risk to which our information assets are exposed. The adoption of this framework will not result in significant additional expenditure with any supplementary funding being met from existing budgets.

COMMENTS OF THE CORPORATE DIRECTOR OF CORPORATE GOVERNANCE

19. The report sets out some of the legal issues which underpin the need for this policy. Most importantly though is the requirement of the Data Protection Act that "appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data". Failure to comply with this principle can result in enforcement action being taken by the Information Commissioner. As Members are data controllers in their own right this policy provides protection to Members individually as well as to the Council as a whole.

COMMENTS OF THE CORPORATE DIRECTOR OF HUMAN RESOURCES AND ORGANISATIONAL DEVELOPMENT

20. The report outlines the new Information Security Framework, which supersedes the previous IT Security Policy. All existing employees and any new employee of the Council will be required to sign that they have read and understood the document prior to being allocated or continuing accessing the Council's ICT system. Any breach of the framework will be subject to disciplinary action.

TIM MURPHY
CORPORATE DIRECTOR (ICT)

There are no background papers to this report.

Report Author	Ext	Date	Doc ID
Tim Murphy	5455	December 2008	ExecCabinetISFReport.doc