INFORMATION SYSTEMS SECURITY POLICY AND COMMUNICATION SYSTEMS ACCEPTABLE USE POLICY

EXECUTIVE MEMBER: Cllr N Williams

LEAD OFFICER: Sue Borwick

REPORT AUTHOR: Chris Lloyd

Summary: This report presents Executive with the Information Systems Security Policy And Communication Systems Acceptable Use Policy for consideration.

Recommendation: Executive is asked to approve the Information Systems Security Policy And Communication Systems Acceptable Use Policy.

Impact on delivering the Corporate Plan: None specifically, but see under Financial and Human resource implications.

Impact on other statutory objectives (e.g. crime & disorder, LA21): The Policy is in line with current legislation, and is intended to reduce incidents of improper use.

Financial and human resource implications: The proposals clarify and regulate the position to be taken by staff using the Council electronic and communications systems. There is no additional funding required.

Project & Risk Management: These proposals set out an acceptable standard for use of electronic communication systems, considerably reducing current risks, and provide a means of effectively dealing with misuse.

Key Decision Status

- Financial: None

- Ward: None

Other Ward Implications: None

1. INTRODUCTION

1.1. A report was presented top the JCSP at its meeting on 17 March 2005, with a recommendation that the Draft Security Policy be noted, and seeking suggestions for any changes to wording etc., that may improve its clarity.

1.2. The panel concluded that it was generally in agreement with the Policy, but would like to see it summarised, and for more detail on Acceptable Use.

1.3. Further work has made it easier to read and follow and has reduced the content without diluting its intent. A separate Acceptable Use Policy has also been provided.

2. POLICY

2.1. The Information Systems Security Policy and Communication Systems Acceptable Use Policy are attached as Appendices A and B which will bring us in line with most other Councils.

2.2. The aim of these policies is to provide clear guidelines as to the way in which all persons must use the Council electronic communications systems. The requirement to follow these guidelines is intended to protect individuals and the Council from the effects of misuse. The electronic communications systems include computers, internet, e-mail, I T storage, mobile and fixed telephones and similar devices.

2.3. The Security Policy is attached for information. It is a comprehensive document covering the full range of issues. The size of the document has been considerable reduced in order to make it as concise as possible.

2.4. The Acceptable use Policy is also attached as a separate document as requirements are of a slightly different nature, more aimed at allowing reasonable personal use and setting out examples of unacceptable use.

2.5 Having a policy should not only be to clarify the Councils policy regarding use of the internet, but also to encourage effective use of the resources and provide a positive direction for their appropriate use:

- It should provide a clear understanding in the use of password, network and office security.
- Provide guidelines to help prevent virus and other malicious attracts directed at the council.
- Provides the Key building blocks for a safe and secure network
- Allows IT to build on an already secure network and extend it safely and securely.
- Provides the guidelines needed to maintain a secure reliable network infrastructure and desktop environment.
- Give IT the guidelines needed to put in place systems and software to provide a safe and secure network.
- Provides the guidelines for configuring, securing and maintaining desktop and laptops leading to standarisation software and ease of maintenance.

In addition the policy allows personal use of the internet and e-mail in own time and within acceptable use as detailed in Appendix B. This was identified as a benefit requested by staff in a recent survey as to what benefits they would like which may help to improve morale and also demonstrate trust.

2.5. Once approved by Executive, the requirements will be fully explained to employees and members who will be required to confirm that they have read and understood them and will abide by them. As with all such Council policies, breach of the Policies could potentially result in disciplinary action.

3. CONCLUSIONS

3.1 Executive is asked to approve the recommendation to approve the Information Systems Security Policy and Communication Systems Acceptable Use Policy.

Appendices:	**Appendix A** Draft Security Policy **Appendix B** Draft Acceptable use Policy
List of Background Documents:	Project file
List of Consultees:	Corporate team. Management Group. Portfolio Holder.