Wi-Fi Policy

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Policy Details
  - Responsibilities

- **Policy Compliance**
  - Document Control

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Wi-Fi Policy

Background

The use of Wi-Fi to connect to the Internet has become an essential business enabler. For some devices, it is the only way they can gain onward access to corporate data and resources.

Whilst corporate devices [iPads, etc.] and services [e.g. Email] are configured to be secure [Passwords, encryption, secure connections], there is still a user requirement to exercise due care in which Wi-Fi connections should be trusted.

Failure to do so will put you and the organisation at risk from data loss, identity theft and reputational damage. This policy document sets out the standards everyone must adhere to when making decisions about the use of Wi-Fi.

Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Key Message

Wi-Fi connections can be classified as one of two types: Direct Connections and Captive Portals.

Direct Connections

The best example of this would be like a home Wi-Fi network provided by your broadband connection. You select the Wi-Fi network, enter any password and connect straight to the Internet.

Captive Portals

These connections take you to a ‘landing page’ [like a registration page] and broker your connection to the Internet.

Whilst the majority of Wi-Fi networks are safe to use, Malicious Actors can and do set up Wi-Fi networks of either type that can try to read your data, exposing you to the risks above. This happens in the UK and abroad; in some foreign countries the deliberate interception of data is a state-sponsored activity.

You must satisfy yourself that the connection is trustworthy, before you connect to it.

Policy Detail

Passwords

Most, but not all, Wi-Fi networks are password protected - this should be considered as a 'network privacy' control and not any guarantee of data security.

Examples of trustworthy Wi-Fi networks

EKS Unify - our 'corporate' Wi-Fi network.

Home Broadband Wi-Fi___33 connections provided by telecoms companies e.g. BT, Virgin, and Sky - reputable companies.

Public Wi-Fi services provided by telecoms companies e.g. VFast, BTOpenzone, O2, and The Cloud. These are good examples of Captive Portal services - where you have to be a member, or take up a subscription.

Other Kent authorities also operate Wi-Fi networks, such as Oakwood House [Speedway] and these are trustworthy.

Examples of non-trustworthy Wi-Fi networks

Web Cafes are non-trustworthy. Whilst this is a broad-brush statement, it represents a reasonable position for data protection needs.

Non-EU countries warrant varying levels of trust, between limited trust [access only non-sensitive data] to no trust [expect all data to be read/stolen].

The same considerations can be extended to wired connections in those circumstances.

Before travelling abroad you should also check your council's policies as regards taking equipment overseas, insurance and accessing data outside of the UK. Consult your line manager for additional guidance.

Responsibilities

You must consider the sensitivity, size and nature of the information being sent or received in determining whether the connection is appropriate before you connect to any Wi-Fi network.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed;

- Councils' disciplinary procedure.
- Breach of contract
- Member code of conduct

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Owner

Document Control		
Title/Version	-	Wi-Fi Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
17/03/2016	Timo Bayford	1.0	Initial Draft for Consideration
24/03//2016	Hannah Lynch	1.1	Amended Version
23/09/2016	CIGG	1.2	Final Review