Business Continuity Policy

- **Introduction**
- **Scope**
- **The Policy**
    - Background
    - Key Messages
    - Risks
    - Policy Detail
    - 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.

Business Continuity Policy

Background

A disaster which prohibits access to the councils premises or severely reduces the available staff would affect critical business procedures, the consequences of which can be severe and include substantial financial loss, an inability to achieve levels of service, embarrassment and loss of credibility or goodwill for the organisation. The consequential damage can have a much wider impact on staff welfare and the general public. The benefit therefore of having a recovery plan that can be implemented with the minimum of delay, will significantly reduce not only the level of disruption, but also the cost of recovering from the disruption, including reducing the cost of reduced productivity to the council, and should ensure the continued confidentiality, integrity and availability of information.

Key Messages

The aim of this policy is to ensure that all information held by the council can be reinstated as soon as possible, ensuring an unbroken level of frontline services, whilst full restoration is planned for and implemented.

The objectives of business continuity planning are to ensure that the council:-

● Understands its critical activities and maintains the capability to resume operations within agreed timeframes, following the deployment of a contingency planning response;

● Increases resilience by protecting critical information assets (electronic and otherwise) through a co-ordinated approach to management and recovery; and

● Minimises impacts using a focused, well-managed response activity.

Risks

- Business and Efficiency
- The Freedom of Information Act
- Data Protection Act/ Subject Access Requests
- Reputational Damage
- Financial Penalties
- Integrity of information

Corporate Information Governance Group
Business Continuity Policy

Policy Detail

The council's policy is to maintain the continuity of its activities, systems, facilities and processes and where these are disrupted by any event to enable it to return to 'normal' operations as soon as possible, taking fully into account the impact of any delay on the council's quality of service, reputation, finances and integrity of information held.

This policy is intended to ensure:

- The concept of Business Continuity and the council's policy and approach is understood by all stakeholders;

- Internal and external dependencies on information in respect of, customers, suppliers, partners and resource implications are identified;

- Individual service business continuity plans are developed to ensure the integrity and future recovery of information in the event of an interruption to services;

- Plans are systematically maintained and tested; and

- a programme of training and communication is put in place.

The Policy assumes a worst-case scenario in which critical information systems and resources are destroyed by fire, other natural events, or by unauthorised entrants committing acts of destruction, theft or sabotage that prevent key service delivery functions being undertaken.

It is assumed that the council's policy as it applies to records management, file management, computer security in general and virus protection in particular, is being applied. Similarly, it also assumes that fire prevention, physical security and health and safety at work standards are also being applied. It assumes that inventories of hardware/software, other business systems and major items of equipment are maintained by Divisions.

Responsibilities

The council should maintain a Business Continuity Plan which includes the responsibility for the continued integrity and safeguarding of the information during the recovery process.

o **Corporate Information Governance Group**

To advise each authority's SIRO, to review the elements of the BCP in respect of information integrity and retrieval for each authority, to effectively manage information and security risks and to monitor and report via the SIROs any security breaches.

o **Senior Information Risk Owner**

The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the Organisation and advises on the effectiveness of information risk management across the Organisation.

o   **Information Asset Owners**

The Information Asset Owner, who should be a system user of appropriate seniority, must ensure that:-

1.   BCP controls are in place, which are appropriate to the sensitivity of the information held.

2.   The major risks which may threaten the confidentiality, integrity and availability of the information are identified and, where possible, mitigated;

3.   The integrity of information is maintained during a BCP event.

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 Officer.

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

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
22/10/2015	Dave Randall Colin Cook	1.0	First Draft for Consideration
23/09/2016	CIGG	1.1	Final Review