ANGUS COUNCIL

INFORMATION SECURITY POLICY

Version:	V02.1
Author:	Angela Dunlop, Project Lead (Information Governance)
Owner:	Lisa Dallas Chief Information Governance Officer
Date of Approval:	23 July 2018
Approved by:	Information Governance Steering Group
Date issued:	23 July 2018
Next review date:	July 2019

Amendment Form

Version	Date	Brief Summary of Changes	Author
1.1	21/8/15	Deletion of list of legislation from Appendix 2 – replaced with generic wording	Shona Cameron
1.2	21/9/15	Finalised Version	Shona Cameron
02	14/10/16	Changes suggested by the RIMWG	Angela Dunlop
02.1	23/07/18	Document updated	Angela Dunlop

CONTENTS

1. POLICY STATEMENT

Information is a vital asset to Angus Council and is an essential element to all of our working. The council recognises the need to ensure that information is processed in a secure manner and is appropriately protected from misuse, unauthorised or accidental modification, destruction, or disclosure by individuals internal or external to the organisation.

Operational procedures will be established to implement the corporate information security requirements outlined in this Information Security Policy, and appropriate mechanisms will be put in place to monitor and manage these procedures.

2. SCOPE

The Information Security Policy applies to **all** information assets which are owned by the council, used by the council in the exercise of its business or which are connected to any networks managed by the council. This security policy also applies to all information which the council processes, irrespective of ownership or form. The information security policy applies to all members of staff, councillors or any others who may process information on behalf of the council.

3. INFORMATION SECURITY PRINCIPLES

The council has previously adopted the following principles, which continue to underpin this policy:-

(1) An information asset is defined to be an item or body of information or an information storage or processing system, which is of value to the council.

(2) Senior Information Officers who form the Information Governance Steering Group will take all appropriate measures to minimise the risks of human error, theft, fraud or misuse of the council's information assets and facilities. Staff will be made aware of information security risks and will receive timely and appropriate information security training.

(3) It is the responsibility of all individuals to handle information appropriately in accordance with council policies.

(4) Information will be processed in line with all relevant council policies and legislation, notably those relating to Data Protection, Human Rights and Freedom of Information.

(5) Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.

(6) Information will be made available solely to those who have a legitimate need for access or where information is released under Freedom of Information or Environmental Information Regulations.

(7) Information will be held securely and will be accurate, adequate, relevant and not excessive.

(8) Information will be protected against unauthorised access.

(9) Business continuity plans will be produced, maintained and tested.

4. COMPLIANCE

All council staff have a responsibility to be aware of, and comply with, the council's policies and procedures and there are various online training materials to support these. Breaches of this Information Security Policy may result in disciplinary action being taken in accordance with the council's disciplinary procedure.

Data protection breaches must be reported in accordance with the Data Protection Breach Protocol:
DP Breach Response Plan

Information Technology security breaches must be reported in accordance with the Information Technology (IT) Security Policy which details the Incident Reporting Procedure therein.

Staff should not attempt to replicate or simulate any suspected security breach or incident. Council staff suspected of deliberately causing a security breach will be subject to investigation under established formal disciplinary procedures.

5. GOVERNANCE

Responsibility for the production, maintenance and communication of this policy document lies with all Senior Information Officers.

This document has been approved by the Information Governance Steering Group and changes or additions to the Information Security Policy may be proposed by any member of staff via their Information Governance Steering Group representative.