**Information Security Policy**

**Introduction**

Information is a vital asset to any organisation, and this is especially so in a knowledge-driven organisation such as Global, where information will relate to learning and teaching, research, administration and management. This policy is concerned with the management and security of Global information assets (an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to Global) and the use made of these assets by its members and others who may legitimately process Global information on behalf of Global.

This overarching policy document provides an overview of information security and lists a hierarchical set of policy documents (sub-policies) which taken together constitute the Information Security Policy of Global.

**Purpose**

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

**Scope**

The documents in the Information Security Policy set apply to all information assets which are owned by Global, used by Global for business purposes or which are connected to any networks managed by Global.

The documents in the Information Security Policy set apply to all information which Global processes, irrespective of ownership or form.

The documents in the Information Security Policy set apply to all members of Global and any others who may process information on behalf of Global.

**Structure**

The Information Security Policy document set is structured in accordance with the recommendations set out in the “UCISA Information Security Toolkit” which in turn, is based on the control guidelines set out in the industry standard ISO 27001.

This top-level document lists a set of other sub-policy documents which together constitute the Information Security Policy of Global. All these documents are of equal standing. Although this policy set should be internally consistent, for the removal of any doubt, if any inconsistency is found between this overarching policy and any of the sub-policies, this overarching policy will take precedence.

 Each of the sub-policy documents only contains high-level descriptions of requirements and principles. They do not and are not intended to include detailed descriptions of policy implementation. Such details will, where necessary, be supplied in the form of separate procedural documents which will be referenced from the relevant, individual sub-policy documents.

**Information Security Principles**

Global has previously (in its original Information Access and Security Policy, 2002) adopted the following principles, which continue to underpin this policy:

1. Information will be protected in line with all relevant University policies and legislation, notably those relating to data protection, human rights and freedom of information.
2. 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
3. Information will be made available solely to those who have a legitimate need for access.
4. All information will be classified according to an appropriate level of security.
5. The integrity of information will be maintained.
6. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
7. Information will be protected against unauthorised access.
8. Compliance with the Information Security policy will be enforced.

**Governance**

Responsibility for the production, maintenance and communication of this top-level policy document and all sub-policy documents lies with Global’s CEO.

This top-level policy document has been approved by Global’s CEO. Substantive changes may only be made with the further approval of the CEO.

Each of the documents constituting the Information Security Policy will be reviewed annually. It is the responsibility of the CEO to ensure that these reviews take place. It is also the responsibility of the CEO to ensure that the policy set is and remains internally consistent.

Changes or additions to the Information Security Policy may be proposed by any member of staff, via their Head of School or Division to the CEO.

Any substantive changes made to any of the documents in the set will be communicated to all relevant personnel.