GISP16. Legal and regulatory compliance

Date:	5 October 2017
Version:	2.0
Authors:	Raymond Scott
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC
1.1	5/10/17	Reviewed and updated
2.0	20/10/17	Approved by ISSC

Policy

Security Control	All use of information systems and assets will comply with current legislation.
Objective	• To ensure that all University IT and computing systems comply with current legislation. • To ensure that information is managed in such a way as to ensure compliance with current legislation. • To ensure that use of the University network is in accordance with regulations of the Joint Academic Network (Janet) and security standards of the Payment Card Industry (PCI).
Policy	16.1. All University IT and computing systems and information services hosted on these must be compliant with current legislation. 16.2. All use of the University network and its connections to the internet must be compliant with Janet regulations. 16.3. All systems connected to the University network falling within the scope of PCI must be compliant with the PCI Data Security Standard (DSS). 16.4. All systems both those run by the University and by third parties which process personal data must be compliant with the expectations of data protection legislation. 16.5. The terms and conditions of the institution provisioning the IT account apply to the use of the account through the host connection, e.g. where an academic visitor uses a UEA connection via eduroam. 16.6. System or service planning process should explicitly define legal obligations. 16.7. The University will have a Records Management Policy and relevant Information Compliance policies. 16.8. A nominated person is responsible for preparing guidelines to ensure that all staff and students are aware of the key aspects of the law of copyright, in so far as these requirements impact on their duties or studies.
Responsibility	• ITCS is responsible for making users, system administrators and data owners aware of legislation and regulations with which they must comply.

	• The Finance Division is responsible for making users, system administrators and data owners aware of PCI regulations with which they must comply. • Individual users are responsible for ensuring their own actions and any systems they are responsible for comply with current legislation and regulations.
Incident Management	Where it is suspected that a computer system, service or activity does not comply with legislation or regulations, the matter should be reported to the owner of the system or service involved. Legal and regulatory breaches should be reported to the Strategy, Policy and Compliance team. For incidents relating to PCI, a defined incident response plan will be followed.
Audit and accountability	The Strategy, Policy and Compliance team are responsible for record keeping, liaison with appropriate authorities and internal departments, and will provide a report on breaches to ISSC on an annual basis.
Implementation	• To support compliance with information legislation, all data owners will ensure that the records held are managed in accordance with the University's records management policy and there exist associated records retention policies and supporting departmental processes to effect them. See https://portal.uea.ac.uk/documents/6207125/7105351/Records-Management-Policy.pdf • Information regulations and policies are available from https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies • All systems that fall within the scope of PCI will adhere to the data security standards required under the relevant PCI SAQ level.