



## Data Protection Policy

1. This Policy sets out the general regulations which govern Southampton Solent University's compliance with the Data Protection Act 1998. The policy is supported by specific protocols and procedures to be followed by University staff, agents, clients, partners and students and should be read in conjunction with other policies, including the E-mail Usage Policy and the Maintenance of Records - Archive Policy. In the case of students, the policy should be read in conjunction with the relevant passages of the **Student Regulations/Charter**. In certain specified instances, these regulations and procedures also apply to clients and associated bodies of the University.

2. The University, its staff, students, clients, agents, and other associated bodies, as Users and/or processors of personal data (computerised and manual), have an obligation to comply with the principles of the Data Protection Act 1998. Under the Act, all individuals, as Data Subjects, have the same rights regarding their personal data.

## Management of Compliance

3. All organisations must notify the Information Commissioner's Office of its intention to process data. The University's correspondent with the Information Commissioner shall be the Deputy Vice-Chancellor or authorised deputy.

4. On a day-to-day basis, the Deputy Vice-Chancellor shall devolve responsibility for Data Protection matters to the Head of Planning, who will review the policy when new legislation, which has an impact on personal data, is brought into force.

5. All contracts with academic partners, vendors, contractors and suppliers must include the University's data protection protocols, which such Data Users must follow.

6. It is the responsibility of all managers to ensure that their staff are aware of this policy and their personal obligations under the Data Protection Act.

7. The Information Management and Compliance Officer, under the management of the Head of Planning, shall ensure that notification under the Data Protection Act 1998, appropriate to all aspects of the University's business, is filed with the Office of the Information Commissioner and is regularly maintained and reviewed, via an annual audit co-ordinated by the Information Management and Compliance Officer.

8. Faculty Registrars and Heads of Service shall ensure that the Information Management and Compliance Officer is made aware of the all personal data held and/or processed within the area of responsibility of their Faculty/School/Centre/Service, and the general nature and purpose of all such data.

9. A rolling programme of audit will be conducted by the Information Management and Compliance Officer and Faculty Registrars /Heads of Service, and individual members of staff shall ensure that management is made aware of any personal data which they may hold and/or process, and any changes to the range of such data since the previous audit.

10. Any new processing of personal data, during the year, should be notified to the Head of Planning and/or the Information Management and Compliance Officer for inclusion in the University's notification.

### Current Notifications

11. The University's statutory obligation to the Office of the Information Commissioner is reflected in the Data Protection notifications renewed on 31/01/08. Relevant code numbers are:

Southampton Solent University	Z5969541
Southampton Solent University Limited	Z6147551

### Code of Practice for Data Users

12. Under the principles of the Data Protection Act 1998 anyone who uses or processes personal data is a 'Data User'. All Data Users (staff, students, partners, clients and agents) have an individual responsibility not only to the University but also to the UK Information Commissioner. Data Users must, therefore, abide by the principles set out in the Act and adhere to the University's Data Protection procedures/guidelines.

### 13. The Data Protection Principles:

- i. Obtain and process personal data fairly and lawfully.
- ii. Obtain and process personal data only for one or more specified and lawful purpose or purposes.
- iii. Personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- iv. Ensure that personal data is accurate and, where necessary, kept up to date.
- v. Hold personal data for no longer than is necessary.
- vi. Process personal data in accordance with the rights of Data Subjects under the Act.
- vii. Take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- viii. Do not transfer personal data to a country or territory outside the European Economic area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.

14. Southampton Solent University may be obliged to comply fully with certain requests made by the Police or other Public Authorities (as stated in the Protection of Children Act 1999, the Terrorism Act 2006, and the Mental Health Act 2007). **Staff should neither confirm nor deny (NCND) if asked for information related to the Terrorism Act. Any such request MUST be sent immediately, in strict confidence, to the Head of Planning or in her/his absence to the Head of the Vice-Chancellor's Office.**