SOLENT UNIVERSITY SOUTHAMPTON	**Title**: **Data Protection Procedures**
	Document Type: Policy
	Location: Policy, Governance and Information Services
	Version: V6
	Publication Date: **July 2021**
	Author: Karen Stephen

1. Introduction

1.1 Solent University ("Solent") processes data for a number of purposes in relation to its staff, students and other individuals who come into contact with the institution. The primary legislation governing the way in which such data should be processed is the **General Data Protection Regulation 2018 ("GDPR") and the Data Protection Act 2018** ("**DPA"**). Solent takes steps to apply the principles of this legislation to all personal data processed.

1.2 **Personal Data ("PD")** is any information relating to an identified or identifiable natural person (**the "Data Subject"**). The Data Subject may be directly identifiable for example, by name or an online identifier (IP address). The Data Subject may be indirectly identifiable if any data element combined with another leads to their identification. For example, a combination of laptop serial number and desk number could identify an individual.

1.3 **Special Category Data ("SCD") also** known as **sensitive personal data** relates to data regarding ethnic or racial origin, political opinions, religious or other beliefs, trade union membership, genetic data, biometric data (where it is used for the purpose of identifying a natural person), data concerning health or data concerning a person's sexual orientation. SCD is subject to greater controls prior to, during and after processing.

1.4 Solent is obliged under the DPA to review any PD (including SCD) that it collects / processes to ensure a lawful basis for data processing is established; sufficient **security, technical and organisational measures** are in place to protect it; and that the Data Subject has received notice or provided consent to Solent's processing of their data.

1.5 Data includes information held as information on a computer, video surveillance and CCTV material, data held on telephone or in paper/manual records. The foregoing is not a finite list.

1.6 Solent provides **staff training** including: induction training; online training modules; training targeted for specific teams; and a refresher course every two years which is compulsory for all employees.

1.7 This policy document applies to Solent employees, agency staff, visitors, contractors and consultants **("Data Users")** who process Personal Data or Special Category Data on behalf of Solent.

1.8 All Data Users who process PD/SCD in connection with Solent must read and comply with this policy and associated documents. **This includes all schools/services/faculties which individually and collectively are also called Data Users**.

1.9 Data Users are obliged to ensure that any PD/SCD which they process is kept securely and not disclosed accidentally or otherwise to any unauthorised third party. In the event of an accidental disclosure please refer to the Incident/Breach Process on the Portal and contact information.rights@solent.ac.uk immediately.

1.10 The Information Commissioner's Office (ICO) is the UK's independent authority in place to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals. Their website https://ico.org.uk/ contains detailed information and guidance about privacy. As well as a source of knowledge, the ICO is the government's regulator. It deals with complaints from individuals and verifies organisations' compliance to the legislation. It has wide powers in the event of non-compliance. These can include financial penalties or in extreme cases, criminal proceedings.

2 Controllers/Processors/Data Protection Officers/Data Subjects

2.1 Data Controller

2.1.1. A Data Controller is the person or organisation which determines the purposes and means of the processing of personal data. Generally, Controllers operate independently and it is possible to have two controllers within one relationship / agreement. It is also legally possible to have "Joint Controllers" although advice must be obtained from information.rights@solent.ac.uk prior to negotiating such an arrangement as it incurs extra burdens for Solent under GDPR.

2.2 Data Processor/Sub-Processors

2.2.1 A Data Processor is any third party who processes Personal Data on behalf of the Data Controller**.** A Processor makes no decisions on how or why to process the data. Data Processors may be able to appoint **Sub-Processors**. The Data Processor is liable for the acts or omissions of their Sub-Processors.

2.2.2 In general, the supplier or other party assumes the role of Processor with Solent as Controller. However, it is possible that Solent could be a Processor where another party acts as Controller. Contact information.rights@solent.ac.uk for advice.

2.3 Data Protection Officer

2.3.1 The current Data Protection Officer ("DPO") is the Chief Operations Officer for Solent University contactable at information.rights@solent.ac.uk. The DPO is responsible for advising Solent and its employees and students about GDPR and its provisions, as well as monitoring compliance with that Regulation.

2.4 Data Subject

2.4.1 A Data Subject is an individual who is the subject of personal information. For example, Sam Doe at samdoe@solent.ac.uk.

2.5 Privacy Notices

2.5.1 A Privacy Notice provides specific details about how the University and its Processors intend to process PD/SCD. The University provides various Privacy Notices on its websites. Privacy Notices may also be presented at the point when PD or SCD is collected.

2.5.2 Solent University has a main privacy notice accessible to staff on the Portal. Specific systems or platforms used by Solent may also have their own privacy notice. Complying with the Data Protection Impact Assessment ("DPIA") process available on the Portal will ensure that an appropriate privacy notice for any new initiative is reviewed and if applicable, executed.

3.Data Protection Principles

3.1 When personal data is processed by the University (manually or electronically), the University has an obligation to comply with the **6 Principles of GDPR**.

3.1 Principle 1: Solent must obtain and process personal data fairly and lawfully.

3.1.1 Solent must have legitimate grounds for collecting or processing PD;

3.1.2 The data collected by Solent must only be used for its original purpose of collection and not for any further purpose.

3.1.5 Personal Data should not be processed unless at least one of these conditions is met:

- the data subject has given **consent** to the processing of his or her PD. Please note, **explicit consent** is specifically required prior to marketing activities (e.g. recruitment) and where SCD is involved;
- processing is necessary for the performance of a **contract** to which the data subject is party;
- processing is necessary for **compliance with a legal obligation;**
- processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the Controller;
- processing is necessary for the purposes of the **legitimate interests** pursued by the Controller or by a third party. This condition has a narrow application and is used sparingly.

3.1.6 For **SCD at least one** of the following conditions must be met

- The Data Subject has given **explicit consent** to the processing;
- Processing is necessary to enable the University to comply with its **legal obligations** under contractual, employment or other applicable law;
- Processing is necessary for the establishment, exercise or defence of **legal claims;**
- Processing is necessary for the purposes of **preventive or occupational medicine;**
- Processing is necessary for **archiving** purposes in the **public interest**, **scientific or historical research** purposes or **statistical** purposes.

3.1 Principle 2: Obtain and process personal data only for one or more specified and lawful purpose or purposes.

3.2.1 Before obtaining Personal Data, Solent must have a clear, legitimate reason for data collection;

3.2.2 On collecting the data Solent will provide a clear and explanatory privacy notice informing Data Subjects of the intended use of their data, keeping in mind that for some initiatives additional steps may be required (e.g. SCD)

3.2 Principle 3: Personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

3.3.1 The amount of personal data held on a Data Subject should not exceed the amount required for its purpose.

3.4 Principle 4: Personal data should be accurate and, where necessary, kept up to date.

Solent must take reasonable steps to ensure the PD it holds is accurate. It should also ensure that a clear record is kept noting the origins of the data: e.g. at enrolment.

3.5 Principle 5: The University should hold personal data for no longer than is necessary.

3.5.1 Regular assessment is undertaken by the University to review the length of time personal data records are held.

3.5.2 Once personal data is no longer required by the University it must be destroyed in an appropriate and secure manner. There are some accepted variations to this, for example certain student records or management records. For legal reasons, a full academic and conduct record should be retained for six years from the date of the student leaving the University. Once that period has elapsed, the record can be reduced to a core record, as holding the data for longer may be considered excessive. A student's results and awards must be kept until the student's retirement age in case Solent needs to produce a copy or evidence of study.

3.6 Principle 6: Appropriate technical, organisational and security measures

3.6.1 All of the University must ensure that Data Security measures are identified, implemented and maintained to protect data and to reduce the potential risk of any data security incident, breach and consequent harm. Periodic reviews must be made of administrative, physical and technical safeguards for protecting Personal Data and Special Category Data held in both paper and computerised form. Where data is stored electronically, Solent routinely reviews and updates its security measures in line with technological advances.

3.6.2 Every precaution is taken to ensure security when transferring personal data in either hardcopy or electronic form. Personal Data should not be stored or processed on laptops or other portable devices unless it is encrypted and only in cases of operational necessity and with a manager's knowledge. For a Guide to Encryption visit the Portal.

3.6.3 Where there is a requirement to transfer SCD between Solent and an external third-party, ensure a DPIA is completed and forwarded as per instructions.

3.6.4 SCD being transferred to third parties must be encrypted.

4. Data Subject Rights

4.1 GDPR sets out a number of rights and freedoms for Data Subjects which must be upheld:

4.1.2 **Right of access** - right to ask for copies of personal information;
4.1.3 **Right to rectification** - right to ask to rectify information that is inaccurate;
4.1.4 **Right to erasure** - right to request erasure of personal information;
4.1.5 **Right to restriction of processing** - right to restrict the processing of information;
4.1.6 **Right to object to processing** - right to object to the processing of personal data.
4.1.7 **Right to data portability** - right to ask that we transfer information to another organisation, or to the data subject in a transferrable format.

4.2 Data Subjects may only enquire about PC/SCD which relates to themselves. This is known as a **Data Subject Access Request ("DSAR")**. The identity of each DSAR will be verified before any information is released. Data about any other identifiable individual is redacted from any DSAR reply.

4.3 There may be certain statutory, confidential commercial circumstances or exceptions which prevent

Solent releasing data. Contact information.rights@solent.ac.uk

5. International Transfers of Data

5.1 Personal data may be transferred to a country or territory in the European Economic Area ("EEA"), and countries that are deemed to have an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.

5.2 The **European Economic Area** consists of the following countries:

Austria	Greece	Netherlands
Belgium	Hungary	Norway
Bulgaria	Iceland	Poland
Cyprus	Ireland	Portugal
Czech Republic	Italy	Romania
Denmark	Latvia	Slovakia
Estonia	Liechtenstein	Slovenia
Finland	Lithuania	Spain
France	Luxembourg	Sweden
Germany	Malta	

5.3 The following **countries/territories outside of the EEA** are currently considered to have an **adequate level of protection** in accordance with GDPR.

Andorra,	Guernsey	New Zealand
Argentina	Isle of Man	Switzerland
Canada	Israel	Uruguay
Faroe Islands	Japan	
	Jersey	

5.4 When a third party in one of the countries/territories in 5.2 or 5.3 will receive or exchange data with the University, it is a legal requirement under the GDPR and DPA that appropriate contractual language is in place to cover this.

5.5 Data may be transferred to / exchanged with third parties in countries not on the above lists. Please complete a DPIA form and notify information.rights@solent.ac.uk for analysis, advice and approval. Such transfers will **always involve the completion of additional Standard Contractual Clauses** or any subsequent mechanism approved for use by the Information Commissioner's Office..

5.6 There are no longer any Data Shield or Safe Harbour Provisions with the United States. For the time being, data transfers to and from the US must be processed under Standard Contractual Clauses (refer to information.rights@solent.ac.uk) .

6.Partners, Agents

Academic partners/collaborators of the University are deemed to be agents of the University and must follow the procedures/guidelines set out in the University's Data Protection Procedures and Guidance Documents.

7.Vendors, Contractors, Suppliers

7.1 University staff must restrict access to Personal Data by non-University employees. Access to data by vendors, contractors and suppliers must be controlled and documented in a binding contract.

7.2 Vendors, contractors and suppliers must be restricted from unnecessary admittance to areas or access to systems where Personal Data is held or processed.

7.3 In all cases where Personal Data will be transferred to or exchanged with vendors, contractors and suppliers, appropriate data sharing agreements must be in place. Refer to the External Data Sharing Policy.

8. Data Incident/Breach

If you suspect or know that there has been an incident which constitute a breach of the privacy or security of Personal Data or SCD either manually, on a system or with one Solent's third party suppliers, notify information.rights@solent.ac.uk. Under current law, the University has 72 (seventy-two) hours to decide whether a data breach is notifiable or not to the Information Commissioners office. Therefore, please do not delay contacting Information Rights. Forms to report Data Incidents and Breaches and guidance on how to handle can be found on the portal.

9. Registration with ICO

The Information Rights & Records Senior Officer shall ensure that registration of the University with ICO under GDPR is updated annually. Solent University Z5969541 / Solent University Ltd Z6147551 / Solent University Services Ltd ZA470174

10. Archiving

Documents should be held in accordance with Principle 5 of the GDPR. For further guidance on document retention please refer to the University's Records Appraisal Guidance, owned by Information Rights.

11. Handling of sensitive & financial personal data

Solent University's policy is that financial information should be handled with the same care as SCD. For example, credit card details should be recorded separately from non-sensitive personal data and only transferred to areas of the University or third parties that are involved in financial processing. Similarly, staff payroll details to be disseminated via e-mail must be encrypted and should never be held on unprotected servers.

12. Publishing Staff Data

It is the responsibility of all members of staff who produce material intended for release into the public domain (e.g. App)that they check the level of permission to release information approved by staff Data Subjects who are featured in the material. All members of staff must ensure that their permissions are up-to-date by going to the following link https://data-preferences.app.solent.ac.uk/

13 CCTV

13.1 CCTV digital images, if they show a recognisable person are considered Personal Data and are covered by GDPR.

13.2 All requests for access to images should be sent to information.rights@solent.ac.uk. Only personnel with direct work responsibilities linked to CCTV image capture or data compliance should have access to such images.

13.3 Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of the data, subject to exemptions contained in the Act. They do not have the right of instant access.

13.4 Individuals who are recognisable from any filming or photography must provide their consent before their image can be shared. If the individual does not consent or cannot be reached to obtain consent, their image must be pixelated.

13.5 The Data Protection Act 2018 gives the University the right to refuse a request for a copy of the data (CCTV image) particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders or affect the privacy of a third party.

13.6 If it is decided that a request should be refused, the reasons must be fully documented and the data subject informed in writing, stating the reasons.

14.Statutory Data Sharing

The University has certain obligations which requires it to share data with statutory bodies, the Students Union and other such organisations. In addition, the University is obligated under the Section 28 (National Security) and Section 29(1)(c) and(3) – (the prevention and detection of crime, or the apprehension, prosecution of offenders and/or the collection of any tax or duty), to provide the police or national security officers with staff/student data, including CCTV images. The police MUST however, provide a fully completed DP2 form at the time of application stating under which section of the DP Act they are requesting the data. Due diligence must be undertaken to verify the validity of the requestor before the release of any information.

15.Contacts and Further Information

Any queries regarding the content of this Policy please refer to the Information Rights & Records Senior Officer reachable at information.rights@solent.ac.uk

Further information about Data Protection matters can be found on the Information Commissioner's website: www.ico.gov.uk