Data Protection Policy

POLICY

POLICY No 07

SSGC DATA PROTECTION

INTRODUCTION

SSGC DATA PROTECTION

The Data Protection Act 1998 ("DPA") gives rights to employees as well as other individuals, about whom information or "data" is obtained or processed, whether manually or automatically (i.e. computer and word processed). The DPA places obligations on education institutions which hold and/or process data about any such individuals.

This document sets out the Company's policy and procedures to meet the requirements of the DPA. It will be made immediately available to all employees and external agencies (having a legitimate interest) upon request, although it is not a substitute for understanding the Act. Additional guidelines will be available for staff. The policy will not be incorporated into contracts of employment.

1. PROCESSING OF DATA

1.1 Data processing within this policy means the obtaining, recording or holding of information or data or the carrying out of any operation using that information or data such as altering or deleting it, consulting it or disclosing it.

1.2 The Company will appoint one or more Data Control Officers as the individuals responsible (whether alone or collectively) for supervising data control and for assisting those processing data to comply with this policy. This person or persons shall also be responsible for notifying the Information Commissioner of the registerable particulars and ensuring that the notification is kept up to date and is amended or reviewed as appropriate. The name or names of the Data Control Officer(s) are recorded in Appendix One. Any person who has access to and processes personal data (referred to in this policy as a data processor) must ensure that he/she complies fully with this policy and with the registerable particulars notified to the Information Commissioner as required under the DPA.

1.3 Where employees are processing personal data as a legitimate part of their employment, they should be able to rely upon the notification to the Information Commissioner provided by the Company. Staff can consult the notification on the Information Commissioner's Web site (http://www.dataprotection.gov.uk/ dprhome.htm).

1.4 It is the responsibility of each individual data processor to ensure his/her familiarity with this policy and the registerable particulars to ensure compliance with the Company's requirements. Further information/ guidance on any aspect of this policy or details of the registerable particulars may be obtained from the Data Control Officer(s).

1.5 Employees should not use Company's facilities to process personal data for purposes unconnected with their employment for domestic or personal purposes. Such processing is not covered by the Company's notification.

2. PURPOSE AND METHOD OF DATA COLLECTION

2.1 The purpose of data collection is to facilitate the processing of data on the Company's employees, organisation structure and other individuals with a relationship to the Company (e.g. suppliers, job applicants, enquirers) and is designed specifically to provide:

2.1.1 Information, whenever required, for planning and managing the Company's activities

Including:
2.1.2 Information, whenever required, for planning, delivering and monitoring the Company's portfolio of services;

2.1.3 Individual information for managing the employment, deployment and welfare of individual employees;

2.1.4 Individual information for managing the attendance, performance and welfare of individual employees;

2.1.5 Information, whenever required, for responding to legitimate external enquiries about the Company's employees

2.1.6 Assistance with personnel and salary administration procedures, e.g. payroll

2.2 The Data Control Officer(s) shall review annually the nature of information being collated or held to ensure there is a sound business reason requiring the information to be held.

2.3 Wherever possible, employees or potential employees should be advised of what personal information/data is obtained or retained, its source, and the purposes for which the data may be used or disclosed. In all cases the individual's consent will be sought. In the main this will be by way of general consent, given at the point at which the information is collected. In the case of personal sensitive data the individual will be asked for his/her explicit consent to the processing of that sensitive data. Sensitive personal data for this purpose includes information relating to an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual orientation or the commission or alleged commission of offences. In the latter case this may include any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court.

2.4 Initial personal data is ordinarily obtained from job application submitted to the Company and thereafter principally from employees themselves, for example through annual appraisal or from requests for information. A statement at the end of the Company's standard job application form clearly outlines that the information collected will be used only for legitimate purposes. A similar statement is also shown on the CDR forms, in this latter case, the information collected being potentially used or referred to for any of the purposes outlined at 2.1 above. A copy of this

policy will be included in the Staff Handbook and on the Intranet.
Employees should not be induced to provide information or be led to believe that a failure to supply information requested by the Company might disadvantage them where this cannot be justified.

3. DISCLOSURE OF DATA

3.1 To ensure compliance with the DPA and in the interests of privacy, employee confidence and good employee relations, disclosure and usage of information held by the Company is governed by the following conditions:

3.1.1 It must be used only for one or more of the purposes specified in the notification and, in the case of documents generated by the Company, (e.g. application forms and appraisal forms) can only be used in accordance with the statement within that document clearly outlining its intended use.

3.1.2 Provided that the identification of individual employees is not disclosed, aggregate or statistical information may be used to respond to any legitimate internal or external requests for data,

3.1.3 Personal data must not be disclosed, either within or outside the Company, to any recipient who is not authorised in the terms of the Data Protection Act, or for any purpose which is not authorised by our notification
3.1.4 Data processors should seek guidance from the Data Control Officer(s) or if any doubt surrounds a request for data, whether internal or external.
NB. External requests for information should be made in writing and data processors should be satisfied about the legitimacy of requests for information and seek valid documentary evidence if appropriate.

3.2 Authorised requests for data by external recipients of data, which do not require the consent of the data subject are:

3.2.1 Requests made for the purposes of law enforcement (i.e. for the prevention or detection of crime, the assessment or collection of any tax or duty or the assessment or collection of any liability via the Child Support Agency). Disclosure is only allowed where failure to make disclosure would be likely to prejudice one of those purposes. In all cases written evidence should be obtained from the Police, Inland Revenue, Customs and Excise and the Child Support Agency (as appropriate) as to the purpose of the request.

3.2.2 Requests in relation to any other compulsory legal processes; again, appropriate written evidence should be obtained beforehand.

3.2.3 Requests, if urgently required, for the prevention of injury and damage to health. If needed to protect the vital interests of the employee, disclosure may be made without prior consent. Otherwise, the written consent of the employee must be obtained beforehand.

3.2.4 Requests made by pension administrators, in order to administer the Company's participation in various external pension schemes.

3.3 Authorised requests for data by external recipients of data, which do require the consent of the data subject are:

3.3.1 Requests from agents authorised by the employee who is the subject of the data, for e.g. mortgage requests, employment references. Confirmation should be sought from the employee/ student, that the information is to be released and, if possible, the employee's written consent should be obtained.

3.3.2 Requests required by authorised officials or representatives of recognised trade unions. Confirmation should be sought from the employee that the information is to be released and, if possible, the employee's written consent should be obtained.
NB All data processors should endeavour to restrict disclosures requested from outside of the Company to those required by law as much as possible and should, at all times follow the Company's security requirements detailed in paragraph 7.

4. ACCURACY OF DATA

4.1 Updating is required only "where necessary" on the basis that, provided the Company has taken reasonable steps to ensure accuracy (e.g. taking up references), data held is presumed accurate at the time it was collated.

4.2 All employees should be made aware of the importance of providing the Company with notice of any change in personal circumstances. The Company has standard forms for updating change of address, telephone number, and those to contact in an emergency, which can be obtained from Division offices and Personnel.

4.3 Standard printouts of personal records will be issued to employees on an annual basis for the purposes of ensuring that the data is up to date and accurate. Employees will be entitled to correct any details although in some cases the Company may require documentary evidence before effecting the correction, e.g. by seeking examination or qualification certificates for amending qualification details.

5. EMPLOYEE'S / STUDENT'S RIGHTS

5.1 Employees are, on receipt of a written request entitled to have access to personal data held upon them which is not excluded data (see paragraph 5.9 below). A fee may be levied for this service (See paragraph 5.8 below). They are also entitled to be informed of the purpose for which the data is or is intended to be used and the likely recipient (or class of recipient).

5.2 Employees are, in addition, entitled to access their own training, and appraisal results and this information will normally be supplied routinely..

5.3 Examiners comments, whether made on the script or in another form are not exempt. Staff should ensure that comments are capable of being reproduced for an employee in a meaningful form.

5.4 Employees will have access to minutes of meetings to which they were involved if available, that contain discussion about them where candidates are named or referred to by identifiers from which they may be identified, unless that data cannot be disclosed without additionally disclosing personal data about a third party.

5.5 Test and appraisal results must not be disclosed to third parties on notice boards or other public places.

5.6 Test and appraisal results should not be given over the phone.

5.7 The Company will comply with a request from an employee Employees will not be permitted access to personal data consisting of information recorded by candidates during an academic, professional or other examination.

5.8 Once an employee makes a request for confirmation of or sight of data held, which must be in writing, the Personnel Department/Division office will refer it to the Data Control Officer(s) to respond promptly on behalf of the Company and in any event before the end of 40 days from the date on which the request was received (subject to paragraph 5.2 above). This is however, conditional upon the Data Control Officer(s) himself/herself being provided with sufficient information to identify the relevant employee and to locate the information sought. The Company is allowed to charge a fee for providing this information of up to £10 for each request. In the case of current employees the Company will waive this charge for the time being. In the case of current employees, the Company reserves the right to charge a fee of £10, depending on the extent of the data requested. In using its discretion, the Company will not be unreasonable. Access to records such as an enrolment form, assessment results, a student transcript will not command a fee.

5.9 The following information is excluded from the above:

5.9.1 Confidential references given by the Company when these relate to the education, training

or employment of staff or employees.

5.9.2 Personal data processed for the purposes of management forecasting or management planning to the extent that disclosure would be likely to prejudice the conduct of that business or activity only.

5.9.3 Personal data which consists of records of the intentions of the Company relating to any negotiations with the employee to the extent that disclosure would be likely to prejudice those negotiations only.

5.9.4 If, in order to comply with a disclosure request, the Company would need to disclose information relating to an identifiable third party then disclosure is not required unless the third party consents or it is otherwise reasonable to comply with the request without such third party consent. If the information sought is a health record and the third party concerned is a health professional who has compiled or contributed to that health record then disclosure should be made.

5.10 In addition to seeking disclosure of information, an employee is also entitled to request that the Company does not process data concerning him/her where this will cause or be likely to cause substantial and unwarranted damaged or distress, either to the employee concerned or to a third party. Such a request will need to be submitted in writing and, where possible, will be agreed by the Company. The employee will not be able to prevent processing, however, if the processing is necessary for compliance with any legal obligation (other than one imposed by contract), it is necessary to protect the vital interests of the employee or is necessary for the performance of a contract to which the employee is a party. Upon receipt of a written request from an employee a Data Control Officer will write to the employee within 21 days confirming that the request will be upheld or giving reasons why it will not.

5.11 Currently, decisions are not made by the Company solely on the automatic processing of data held. Should, in future, any decision be taken on this basis which significantly affects an employee (or prospective employee/ student) then a Data Control Officer must notify that employee that the decision was taken on that basis as soon as reasonably practicable together with the logic for that decision making. The employee or student applicant is then entitled, within 21 days of receiving that notification, to submit a written request that that decision be reviewed. The Data Control Officer, upon receiving such a written request, will then have 21 days to respond. This right only applies where there has been no exercise of human judgement whatsoever.

5.12 An employee who feels that he/she has, or is likely to suffer damage as a result of either inaccuracy in the data held by the Company or as a result of unauthorised disclosure of information must notify a member of the Personnel Department/Division office in writing immediately. Where appropriate, the Company will correct or erase that information or indicate

that the information is contested by the employee.

5.13 Employees/employees have a number of remedies open to them through the Courts in the event that this policy or their legal rights in respect of personal data are not complied with. In all cases however, employees should use the official Complaints Procedure published in their student handbooks, whilst Employees should use the Grievance Procedure.

5.15 In some cases personal data is held by Client organisations. The Company looks upon these organisations as an autonomous body and in such capacity the Company expects these organisations to be responsible for the registration of personal data.

6. TRANSFER OF DATA OUTSIDE THE UK

6.1 It is a requirement of DPA that personal data shall not be transferred to any country or territory outside of 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.

6.2 For the avoidance of doubt the European Economic Area currently includes Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden and UK. The employee is, however, able to consent to the transfer of data in circumstances where the transfer is necessary.

6.3 The Company will seek the explicit consent employee, if it becomes necessary to process and transfer data relating to that employee to a country or territory outside the European Economic Area.

7. SECURITY

This policy is designed to fulfil statutory requirements and to prevent unauthorised disclosure of/or access to personal data. The following security measures will therefore be required in respect of the processing of any personal data.

7.1 Access to personal data on employees is restricted to those members of staff who have a legitimate need to access such data in accordance with the Company's notification to the Information Commissioner.

7.2 Members of staff authorised to access personal data under paragraph 7.1 above, will be allowed to do so, only in so far as they have a legitimate need and only for the purposes recorded in the notification

7.2 All persons processing data and individuals requesting access to personal data in

accordance with this policy must have familiarised themselves with this policy and it will be the task of the Data Control Officers to ensure that all such personnel are thoroughly trained in its use.

7.3 Access to computer held data is subject to the same restrictions as above save that all staff authorised to access personal data will be required to have passwords in order to access the data. These passwords will be changed at regular intervals to ensure security is maintained. Disclosure of a password to any other employee could result in a formal disciplinary investigation.

7.4 All personal data will be stored in such a way that access is only permitted by authorised staff. This includes data stored in filing cabinets and other storage systems. Acts or omissions by employees which lead to unauthorised access or disclosure could lead to a formal disciplinary investigation.

7.5 Personal data should be transferred under conditions of security commensurate with the anticipated risks and appropriate to the type of data held.

7.6 Personal data held electronically should be appropriately backed up and stored securely to avoid incurring liability to individuals who may suffer damage or distress as a result of the loss or destruction of their personal data.

7.7 Any disposal of personal data will be conducted in a secure way, normally by shredding or security waste. All computer equipment or media to be sold or scrapped must have had all personal data completely destroyed, by re-formatting, over-writing or degaussing.

7.8 In the case of unauthorised or unlawful processing of personal data, appropriate technical and organisational measures will be undertaken.

7.9 In the case of accidental loss, damage or destruction of personal data, appropriate technical and organisational measures will be employed.

7.10 Personal data shall only be kept for as long as is necessary for those specific purposes for which it was obtained, and not used for any other purposes that are incompatible with the original purpose for acquiring it.

8. THIRD PARTIES

8.1 Any personal data which the Company receives and processes in relation to third parties, such as visiting academics, suppliers, former employees, employers, enquirers and other individuals on mailing lists etc. will be obtained lawfully and fairly and dealt with in accordance with the principles and conditions of the Act.

8.2 Employees should ensure that in all cases the use to which the data is to be put is registered in the Notification (See 1.4)

8.3 Employees should obtain explicit consent from third party data subjects to process such personal data for the purposes expressed in the Notification and should ensure that there is a mechanism for data subjects to gain access to data about themselves, to prevent the processing of such data for the purposes of direct marketing and to object to the disclosure of such data.

8.4 In cases in which it is necessary to transfer personal data relating to a third party to a country or territory outside the European Economic Area, the data processor should seek advice from the Data Control Officer in order to satisfy himself/herself that such country or territory has security measures for the protection of data at a standard at least equivalent to the United Kingdom. The data subject is, however, able to consent to the transfer of data in circumstances where the transfer is necessary.

9. Student use of Personal Data held by the Company is not permitted.

10. CONTRACTORS AND SUPPLIERS

10.1 In certain circumstances it may be necessary to allow contractors or suppliers access to personal data in the course of maintenance or repair work.

10.2 In such circumstances, contractors should be documented and wear some form of identification. They should be restricted from unnecessary admittance to areas where personal data is held or processed and, if necessary, required to sign nondisclosure agreements, if access to personal data is unavoidable.

11. STAFF USE OF PERSONAL DATA OFF-SITE, ON HOME COMPUTERS OR AT REMOTE SITES

11.1 Employees processing personal data off-site should ensure they take reasonable precautions to prevent the data from being accessed, disclosed or destroyed as a result of any act or omission on their part. They should notify the Data Protection Officer immediately in the event of theft.

12. USE OF PERSONAL DATA IN RESEARCH

12.1 The 1998 act provides certain exemptions for 'research purposes' including statistical or historical purposes.

12.2 Provided that the purpose of research processing is not measures or decisions targeted at particular individuals and it does not cause substantial distress or damage to a data subject, then personal data may be:

i. Processed for purposes other than for which they were originally obtained
ii. Held indefinitely
iii.Exempt from the right of access by data subjects where the results do not identify individual data subjects

12.3 Most of the Data Protection Principles still apply to personal data used for research purposes and researchers should always provide clear guidance to individuals whose personal data will be used in research as to why the data is being collected and the purposes for which it will be used.

13. COLLECTION OF PERSONAL DATA FROM WEB PAGES

13.1 The Company will provide the following information on any Web pages designed to collect personal data:

i. The purpose for which the data is being collected

ii.The recipients or classes of recipients to whom the data may be disclosed

iii. An indication of the period for which the data will be kept

iv. Any other information to ensure that the processing is 'fair'

13.2 The Company will provide users with the opportunity to opt out of any parts of the collection of or use of the data that are not directly relevant to the intended transaction