

DATA PROTECTION POLICY

Introduction

SCFEC needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that members of staff can be recruited and paid and, courses organised, and to comply with legal obligations to funding bodies and government. To comply with the law, information must be collected and used fairly, stored safely, not disclosed to any other person unlawfully, and destroyed securely as soon as its retention can no longer be justified. To do this, SCFEC must comply with the Data Protection Principles, which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- be adequate, relevant and not excessive for those purposes
- be accurate and kept up to date
- not be kept for longer than is necessary for that purpose
- be processed in accordance with the data subject's rights
- be kept safe from unauthorised access, accidental loss or destruction
- not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

SCFEC and all members of staff or others who process or access any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, SCFEC has developed this Data Protection Policy.

Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by SCFEC from time to time. Any failure to follow the policy can, therefore, result in disciplinary proceedings.

The Board of Governors is ultimately responsible for the content of this Policy and its subsequent implementation. The Policy has been accepted by the Board of Governors at its meeting on 18 July 2006 and the Policy will be reviewed by the Board of Governors as part of its cyclic process of reviewing all SCFEC policies.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

Definitions

A Data Subject is the living individual who is the subject of the personal information (data).

A Data Object is an item of information of data i.e. name, address, date of birth. In this respect it can also be referred to as Personal Information

A Data User is a person authorised by SCFEC to access and process information about a Data Subject

Sensitive information, as defined by the Data Protection Act, is that relating to: ethnicity; political opinions; religious beliefs; trade union membership or non-membership; physical or mental health; sex life or criminal records. The data subject must give express consent to the processing of such data, except in genuine emergencies. Information required to monitor equal opportunities or socio-economic trends is already collected, under stringent conditions, by the relevant departments in the central administration. It is unlikely that other departments need to undertake similar exercises (if departments think they need to collect any of these details, they should first contact the Data Protection Manager).

Notification of Data Held and Processed

All members of staff, students and other users are entitled to:

- know what information SCFEC holds and processes about them and why
- ensure that this information is current and be given the opportunity to check and correct it on a regular basis.

SCFEC will therefore provide all members of staff, students and other relevant users with a pro forma Schedule of Information Held at least once a year and give each recipient the opportunity to notify amendments by writing on the notification and returning it to a specified area. Amended schedules will be re-issued within 1 month to show that the changes have been implemented.

Responsibilities of Members of Staff

All members of staff are responsible for:

- checking that any information that they provide about themselves to SCFEC in connection with their employment is accurate and up to date
- informing SCFEC of any changes to information, which they have provided. changes of address
- checking the Schedule of Information Held that SCFEC will send out to them each year, and informing SCFEC of any errors or changes
- attending all Data Protection training and seminars as required from time to time by the SCFEC as their employer.

SCFEC cannot be held responsible for any errors unless the staff member has informed SCFEC of them.

Data Security

The Employer is responsible for ensuring that:

- equipment, secure electronic systems and storage are provided to facilitate the requirements of the Data Protection Act
- regular training and briefings on data protection is provided for staff
- new staff are informed of their responsibilities at induction
- the corporation's Data Protection Policy is available on the Staff Intranet.

Each member of staff is responsible for ensuring that:

- any personal data, which they hold, is kept securely
- personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party
- they have satisfied themselves that the person(s) to whom they are considering giving such information is who they claim to be and that they are entitled to the information they are requesting.

If and when, as part of their responsibilities, members of staff collect information about other people (e.g. about students' course work, opinions about ability, references to other academic institutions or details of personal circumstances), they must comply with the Staff Guidelines for Data Protection, which are included as an appendix to this document.

Members of staff should note that unauthorised disclosure will usually be treated as a disciplinary matter, and may be considered gross misconduct in some cases. In all cases of doubt, reference must be made, in writing, to the Data Protection Officer or the Data Protection Manager before the information is divulged. Members of staff are advised that, under certain circumstances, the fact that a named person is employed by or is a student of SCFEC may itself be a matter of confidence.

Personal information must be:

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or
- kept only on removable media which is itself kept securely.

Student Obligations

Students must ensure that all personal data provided to SCFEC is accurate and up to date. They must ensure that changes of address, etc are notified to the student registration office as soon as possible.

Rights to Access Information

Members of staff, students and other users of SCFEC have the right to access any personal data being kept about them either on computer or in *any* formal or informal files. Any student who wishes to exercise this right should complete a SCFEC Access to Information form and hand it to the Director of Student Services. Any member of staff who wishes to exercise this right should complete the form and give it to the Personnel Officer. The Access to Information form can be obtained from Data Protection Manager.

SCFEC will normally make a charge of £10 on each occasion that access is requested, although SCFEC has discretion to waive this.

SCFEC aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is good reason for the delay. In such cases, the reason for the delay will be explained in writing to the data subject making the request.

Publication of SCFEC Information

Information that is already in the public domain is exempt from the 1998 Act. It is SCFEC policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- names of SCFEC governors
- list of members of staff
- photographs of key staff.

SCFEC's internal phone list will not be a public document.

Any individual who has good reason for wanting details in these lists or categories to remain confidential should contact the Personnel Officer.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race or ethnic origin or other sensitive information. There are a number of reasons for this including:

- to ensure that SCFEC is a safe place for everyone
- to operate policies such as sick pay or equal opportunities
- to comply with Children Act obligations
- to comply with other enactments to ensure that members of staff are suitable for the job and students for the courses offered.

Members of staff and students (prospective or current) can be asked to give explicit consent for SCFEC to process certain information regarded as sensitive. A refusal to give consent can result in any offers of employment or course places being withdrawn.

The Data Controller and the Designated Data Controller/s

SCFEC as a body corporate is the data controller under the Act, and the Board of Governors is therefore ultimately responsible for implementation. However, the designated data controllers will deal with day-to-day matters.

The designated data controllers are Urmila Rasan (Data Protection Officer), Archie Foulds, Mac Paton, Susan Stebbings, David Knowles, Terry Stevens, Debbie Campana and Pam Langdon-Pratt. Technical advice on Data Protection issues is provided by Martin Carr who is designated Data Protection Manager.

Release of Sensitive Information

As indicated previously, it is expressly forbidden for any member of SCFEC staff to provide details of any other member of staff or any student to any person or organisation during an incoming telephone conversation. (This does not affect the exchange of information about students or members of staff between members of staff.) All requests for such information from external organisations, including the Police, Home Office etc must be in writing, ideally using the form prepared for the purpose by the Metropolitan Police. Where speed is of the essence, this form may be faxed to the college and the response may be faxed back, but, in the latter case, the responding officer is responsible to ensure, by telephone communication, that the person requesting the information is present at the receiving fax machine so that the material provided is not left in an open office environment.

Where parents, or students, telephone to request information, the request **MUST** be refused on the grounds of Data Protection. Information of this nature can only be provided to the student, face-to-face, to ensure that the correct person is receiving the information. The presence of a second person at such a meeting may be taken as tacit agreement of the Data Subject that this information may be shared with the accompanying person.

Particular care must be taken when dealing with requests for references in respect of both members of staff and students. All such requests will be treated with suspicion unless accompanied by an authority signed by the Data Subject. Where an authority signed by the Data Subject has not been provided, the Data Subject will be approached to provide one before any information of any nature is released. This includes any indication (verbal as well as written) that a person is a member of staff or a student of SCFEC.

Nothing in the paragraph may be taken to affect the responsibility of the SCFEC to provide information about members of staff or students to specific ruling and/or Government bodies e.g. Inland Revenue, DfES etc.

Retention of Data - Students

SCFEC will keep some forms of information about students longer than others. In general, information about students will be kept for a maximum of five years after they leave the SCFEC. This will include:

- name and address
- academic achievements, including marks for coursework and
- copies of any reference written.

All other information, including any information about health, race or disciplinary matters will be destroyed within 2 years of the student leaving SCFEC.

Retention of Data - Members of Staff

In general, all staff information will be kept for six years after a member of staff leaves the SCFEC. Some information, however, will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment and information required for job references. A full list of information with retention times is available from the appropriate data controller.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of SCFEC. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to SCFEC facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the appropriate data controller.

APPENDIX TO THE DATA PROTECTION POLICY

Staff Guidelines for Data Protection

1. Members of staff will process data about students on a regular basis, when marking registers, or SCFEC work, writing reports or references, or as part of a pastoral or academic supervisory role. SCFEC will ensure, through registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 1998 Act. The information that members of staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

- general personal details such as name and address
- details about class attendance, course work marks and grades and associated comments
- notes of personal supervision, including matters about behaviour and discipline
- examination results.

2. Information about a student's physical or mental health, sex life, political or religious views, trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student's consent. If members of staff need to record this information, they should use the SCFEC standard form which can be found on the Staff Intranet.

Examples of such information would be recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties.

3. All members of staff have a duty to make sure that they comply with the data protection principles, which are set out in the SCFEC Data Protection Policy. In particular, members of staff must ensure that records are:

- accurate
- up-to-date
- fair
- kept and disposed of safely, and in accordance with the SCFEC policy.

4. SCFEC will designate a member of staff in each area as 'authorised staff'. These members of staff are the only ones authorised to hold or process data that is:

- not standard data
- sensitive data.

The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary;

- in the best interests of the Data Subject; AND

- the non-authorized staff member has either informed the authorized person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances

This should only happen in very limited circumstances, e.g. a student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student is pregnant or a Jehovah's Witness.

5. Authorized staff will be responsible for ensuring that all data is kept securely.
6. Members of staff shall not disclose personal data to any other staff member, unless for normal academic, administrative or pastoral purposes, except with the authorisation or agreement of a designated data controller, or in line with SCFEC policy.
7. Before processing any personal data, members of staff should consider the checklist below.

Staff Checklist for Recording or Processing Sensitive Data

- Have you read and understood the Dos & Don'ts poster?
- Have you attended a Data Protection training course?
- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?
- Have you reported the fact of data collection to the authorised person within the required time (i.e. not more than 2 weeks)?

APPENDIX TO THE DATA PROTECTION POLICY

Responsibilities

1 RESPONSIBILITIES OF SCFEC AS AN EMPLOYER.

SCFEC is responsible for ensuring that:

- equipment, secure electronic systems and storage are provided to facilitate the requirements of the Data Protection Act
- regular training and briefings on data protection is provided for staff
- new staff are informed of their responsibilities at induction
- the corporation's Data Protection Policy is available on the Staff Intranet.

2 RESPONSIBILITIES OF MEMBERS OF STAFF AS EMPLOYEES.

Staff are responsible for:

- checking that any information that they provide about themselves to SCFEC in connection with their employment is accurate and up to date
- informing SCFEC of any changes to information, which they have provided. changes of address
- checking the Schedule of Information Held that SCFEC will send out to them each year, and informing SCFEC of any errors or changes
- attending all Data Protection training and seminars as required from time to time by the SCFEC as their employer..

3 RESPONSIBILITIES OF MEMBERS OF STAFF AS OFFICIALS WITHIN SCFEC.

Staff are responsible for ensuring that:

- any personal data, which they hold, is kept securely
- personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party
- they have satisfied themselves that the person(s) to whom they are considering giving such information is who they claim to be and that they are entitled to the information they are requesting.

Martin Carr
Data Protection Manager
July 2006