INTRODUCTION
Like all educational establishments, the College holds and processes information about its Fellows, employees, applicants, students, alumni and other individuals for various purposes (for example, the administration of the admissions process, the effective provision of academic and welfare services, to record academic progress, to operate the payroll and to enable correspondence and communications including the provision of references and certificates).

To comply with data protection law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. This Policy, so far as it is relevant, applies to personal information kept in manual or computerised files, whether or not those files comprise a relevant filing system, and therefore fall within the ambit of the Data Protection Act.

The Data Protection Act 1998 ("DPA98") came into force on 1 March 1998. Its purpose is to limit and safeguard the storage and use of personal data (i.e., information about living, identifiable persons). All holdings of personal data fall under the aegis of DPA98, unless they are maintained purely for personal use. The information and guidelines within this policy therefore apply to the entire College: the Master, Fellows and all staff and students (referred to collectively as the "College").

SUMMARY OF AIMS
The lawful and correct treatment of personal information is vital to successful operations, and to maintaining confidence in the College and the individuals with whom it deals. Therefore, Sidney Sussex College commits itself to:
- observing fully conditions regarding the fair collection and use of information;
- meeting its legal obligations to specify the purposes for which information is used;
- collecting and processing appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensuring the integrity of information used;
- applying strict checks to determine the length of time information is held;
• ensuring that the rights of people about whom information is held can be fully exercised under the Act (these include the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; and the right to correct, rectify, block or erase information which is regarded as incorrect);
• taking appropriate security measures to safeguard personal information;
• ensuring that personal information is not transferred abroad without suitable safeguards.

NOTIFICATION TO THE INFORMATION COMMISSIONER
The College has an obligation as a Data Controller to notify the Information Commissioner of the purposes for which it processes personal data. Individuals can obtain full details of the College's data protection register entry with the Information Commissioner from the College Data Protection Officer or from the Information Commissioner's website (www.dataprotection.gov.uk).

DATA PROTECTION OFFICER
The College Data Protection Officer is the Senior Tutor. All queries about the College policy and all requests for access to personal data should be addressed to the Data Protection Officer.

DATA PROTECTION PRINCIPLES
The College, as a Data Controller, must comply with the Data Protection Principles, which are set out in DPA98. In summary these state that personal data shall:
• be processed fairly and lawfully and shall not be processed unless certain conditions are met.
• be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes.
• 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 those purposes.
• be processed in accordance with the data subject’s rights under DPA98.
• be kept safe from unauthorised or unlawful processing, accidental loss or destruction.
• not be transferred to a country outside the European Economic Area, unless that country or territory has equivalent levels of protection for personal data.

DATA SECURITY AND DISCLOSURE
All members of the College and staff are responsible for ensuring that:
• any personal data that they hold is kept securely.
• personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party, and that every reasonable effort will be made to see that data is not disclosed accidentally.

Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct. If in any doubt, consult the College Data Protection Officer. Personal data must be
• kept in a locked filing cabinet, drawer or room; or
• if the data is computerised, be password protected or kept only on disk which is itself kept securely; or
• subject to any other appropriate security measures in addition to those above.

In addition to the requirements of the Data Protection legislation, the confidentiality of information about individuals must be respected.

PROCESSING
"Processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:
• organisation, adaptation or alteration of the information or data,
• retrieval, consultation or use of the information or data,
• disclosure of the information or data by transmission, dissemination or otherwise making available, or
• alignment, combination, blocking, erasure or destruction of the information or data.

RESPONSIBILITIES OF DATA USERS
All members of the College who record and/or process personal data in any form are termed Data Area Contacts. All Data Area Contacts must ensure that they comply with the requirements of DPA98 (including the Data Protection Principles) and with the College’s data protection policy (including any procedures and guidelines which may be issued from time to time). This means that all Data Area Contacts must take steps to ensure that they do not process any data unless they have a legitimate purpose for doing so. This includes reviewing all records currently held that relate to either former or current staff and students and adopting as best practice a system which means that no records are held/stored unless absolutely necessary, making sure that files do not contain anything that the College would be unhappy or embarrassed to have to show to the individual to whom it related, and considering what arrangements need to be put in place to ensure that consent is gained from the subject for any of his/her data that you do hold. A breach of the 1998 Act and/or the College's Data Protection Policy may result in disciplinary proceedings.

In addition, all members of College must register any computer systems and manual filing systems that are used for processing personal data with the Data Protection Officer, indicating for each of them what type of personal data is held and the purpose for which it is processed; a copy of the survey sheet to be used for the purpose is attached (DP Form B).
Thereafter, no member of the College may, without prior written notification to the Data Protection Officer:

- develop a new computer system for processing personal data;
- use an existing computer system to process personal data for a new purpose;
- create a new manual filing system containing personal data;
- use an existing manual filing system containing personal data for a new purpose.

The above does not apply to databases which are maintained by individual Data Area Contacts within the College for their private domestic uses, e.g., private address books. However, individual Data Area Contacts have a responsibility to consider whether their private domestic uses fall within the scope of DPA98.

"DATA HOLDINGS" AND "DATA AREA CONTACTS"

To aid the efficient administration of the College's data protection policy, the data that the College holds/processes has been divided into a number of "Data Holdings": these are described below, showing who may have access to the data. In each case, there is also a specified Data Area Contact. He or she will be responsible in relation to the data in the Data Holdings in question (and thus not simply for the files which he or she maintains) for the following:

- informing the Data Protection Officer of proposed processing of personal data within College which may need to be notified to the Information Commissioner
- providing personal data to the Data Protection Officer in response to a subject access request when requested to do so by the Data Protection Officer
- maintaining the security of, and access to, personal data within the Data Holdings.

From time to time other Data Holdings and/or Data Area Contacts may be designated.

SENSITIVE PERSONAL DATA

The College may from time to time process "sensitive personal data" relating to admissions candidates, members and staff of the College. "Sensitive personal data" is information as to a data subject’s racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, offences or alleged offences, and information relating to any proceedings for offences committed or allegedly committed by the data subject, including the outcome of those proceedings. Currently, the College envisages the need to process sensitive personal data of a type specified in the consent forms set out in Annex A to this policy for the purposes specified. For example, data relating to the ethnic origin of members or staff of the College may be processed for the purposes of equal opportunities monitoring or to identify any necessary dietary requirements and possible sources of financial assistance. Medical records need to be processed for the provision of healthcare and general welfare, to identify any necessary dietary and accommodation requirements and to assist in meeting the needs of members of the College with disabilities. In exceptional circumstances, the College may need to process information regarding criminal convictions or alleged offences in
connection, for example, with any disciplinary proceedings or other legal obligations. In other circumstances, where sensitive personal data is to be held or processed, the College will seek the explicit consent of the member of the College in question unless one of the limited exemptions provided in the DPA98 applies (such as to perform a legal duty regarding employees or to protect the data subject's or a third party's vital interests).

**CANDIDATES' AND STUDENTS' OBLIGATIONS**
Candidates and students must ensure that any personal data provided to the College is accurate and up to date. They must ensure that any changes of address or other personal details are notified to the Admissions Director or his staff in the case of candidates, or the Senior Tutor or his staff in the case of resident students. Students must comply with the College’s policy concerning the security of personal data held on computers (see below).

**DATA SUBJECTS' CONSENT**
Certain types of personal data may be processed for particular purposes without the consent of individual data subjects. However, it is the College’s policy to seek express consent whenever practicable from individual data subjects for the main ways in which the College may hold and process personal data concerning them. This is to allow individuals an opportunity to raise any objections to any intended processing of personal data. The College will consider any such objections but reserves the right to process personal data in order to carry out its functions as permitted by law. Therefore, all prospective Fellows, staff, admissions candidates and students will be asked to sign a consent form regarding particular types of information which the College may in due course hold/process about them. Existing Fellows, staff and students will also be asked to sign a consent form (to follow).

**RIGHT TO ACCESS PERSONAL DATA**
Staff, students and other individuals have the right under the 1998 Act to access any personal data that is being held about them either in an “automatically processable form” (mainly computer records) or in a “relevant filing system” (i.e. any set of information structured in such a way that specific information relating to a particular individual is readily accessible) and to request the correction of such data where they are incorrect. An individual who wishes to exercise his/her right of access is asked to complete the College “Subject Access Request” form (DP Form A - attached) which is available from the Senior Tutor’s Secretary and return it to the Data Protection Officer. Any inaccuracies in data disclosed in this way should be communicated immediately to the Data Protection Officer who shall take appropriate steps to make the necessary amendments. The College will make a charge of £10 (or such other charge as is permitted from time to time by the DPA98) on each occasion that access is requested and this fee should accompany the Subject Access Request form. In accordance with DPA98, the College reserves the right to refuse repeated requests where a reasonable period has not elapsed between requests. The College will normally respond to the request for access to personal data within 40 days (including bank holidays and weekends) of the request or payment of the fee, whichever is the later. The
provisions of DPA98 with respect to individuals’ access rights came into effect fully on 23 October 2007. The Freedom of Information Act 2000 gives individuals extended rights of access in certain circumstances to information which is not held on computer or in a relevant filing system. Please contact the Data Protection Officer for further information.

PROTECTION OF DATA HOLDINGS

**Tutorial files.** Tutorial files are maintained in respect of students' academic progress and welfare. They may also contain financial and medical data. The purposes for which they are maintained include the relevant student’s applications for employment, professional training or admission to other educational establishments. Current Tutorial files are to be kept by the Senior Tutor and the relevant Tutors. Tutorial files may be consulted on a day-to-day basis by the Senior Tutor and, where appropriate, the Admissions Director, Graduate Tutor, Dean, the student's own Director of Studies or Personal Tutor, and/or their secretaries. All other requests for access to a Tutorial file must be authorised by the Senior Tutor.

*Data Area Contact: Senior Tutor/relevant Tutor*

**Student admissions files.** Admissions files are maintained in respect of candidates, and potential candidates, for admissions. During the admissions process such files are maintained and kept by the Admissions Director, or the Graduate Tutor and their staff. For successful candidates, the admissions documentation is included in a tutorial file. For unsuccessful candidates, the admissions documentation is retained for one year and then destroyed. During the admissions process, Admissions files may be consulted by the Senior Tutor/Graduate Tutor (as appropriate) the Admissions Director, any Director of Studies and any other interviewers. All other requests for access to an Admissions file must be authorised by either the Admissions Director or the Graduate Tutor.

*Data Area Contact: Admissions Director/Graduate Tutor*

**Files relating to loans and grants made by the College to students.** These are maintained and kept by the Senior Tutor and Student Finance Officer. The files may be also be consulted on a day-to-day basis by the Graduate Tutor, the Bursar, their secretaries, the College Accountant, and appropriate staff in the College Office. All other requests for access to any of these files must be authorised by the Senior Tutor for those held by him and the Bursar for those held in the College Office.

*Data Area Contact: Senior Tutor/Bursar*

**Files in respect of any disciplinary matters involving students.** All such files are to be maintained and kept by the Dean. Sensitive information is to be placed in a sealed envelope in the student’s Tutorial File. All other requests for access must be authorised by the Dean or Senior Tutor.

*Data Area Contact: Disciplinary Dean*

**Medical files in respect of health and welfare of Fellows, staff and students.** Medical files are to be maintained and kept by the College Nurse. All other requests for access to medical files must be authorised by the College Nurse.
Medical notes in respect of students. Such notes are maintained by the Senior Tutor for health and safety reasons to assist in meeting the needs of students with disabilities, or for reasons connected with absences from College, poor performance, applications to the University or to charities etc. All current notes in this category are to be kept by the Senior Tutor. Sensitive information is to be placed in a sealed envelope in the student's Tutorial File. The notes may be consulted on a day-to-day basis by the Senior Tutor and the Senior Tutor's secretary. All other requests for access to these notes must be authorised by the Senior Tutor.

Data Area Contact: College Nurse

Files relating to Fellowship competitions. These are maintained and kept by the Master’s secretary. These files may be consulted on a day-to-day basis by the Master and her secretary. All other requests for access must be authorised by the Master.

Data Area Contact: Senior Tutor

Personnel files in respect of Fellows. Files relating to Fellows are maintained and kept by the Master’s PA and the Bursar. These files may be consulted on a day-to-day basis by the Master, the Vice-Master, the Bursar and their secretaries. All other requests for access to any of these files must be authorised by the Master and/or the Bursar.

Data Area Contact: Master

Personnel files in respect of other employed staff of the College. These are maintained and kept by the Human Resources Manager. These files may be consulted on a day-to-day basis by the Bursar, the Domus Bursar, the Bursar’s Secretary, Payroll Officer and the relevant Head of Department. All other requests for access to these files must be authorised by the Bursar or Domus Bursar.

Data Area Contact: Master/Bursar

Wages files in respect of employed staff and Fellows. All files relating to payments of wages, stipends or fees are maintained and kept by the Payroll Officer, and can be accessed by the Bursar, HR Manager & College Accountant. All other requests for access to these files must be authorised by the Bursar or HR Manager as appropriate.

Data Area Contact: HR Manager/Bursar

Files relating to Fellows and students maintained by College Librarian. These are maintained and kept by the College Librarian to record the whereabouts of library books. These files may be consulted on a day-to-day basis by the College Librarian and her assistant. All other requests for access must be authorised by the College Librarian.

Data Area Contact: College Librarian

Files relating to tenancies of College properties, suppliers of goods and services to the College, and other third parties not otherwise dealt with in this policy document. These are maintained and kept by the College Accountant, Bursar, the Domus Bursar, the Bursar’s...
Secretary and the Housekeeper. These files may be consulted on a day-to-day basis by the Bursar, the Domus Bursar, the Bursar’s Secretary, the Housekeeper, the College Accountant, and [College Office staff]*. All other requests for access must be authorised by the Bursar, the Domus Bursar or the College Accountant.

**Data Area Contact:** College Accountant

**Alumni Relations and Development.** Manual and computer based files are maintained in respect of current and former Fellows, non-resident members, and other current, past and potential donors to the College. All manual files are to be kept in the locked Development Office; access to the computer database is to be password protected. Development Office staff may consult the manual and computer based files on a day to day basis, but requests by others to view the manual files must be authorised by the Membership and Events Officer, unless they are already an authorised user of the Development Office database. Data will be used by the College for a full range of non-resident member activities, including the sending of College publications, promotion of benefits and services available to non-resident members (including those being made available by external organisations), notification of non-resident member activities and fund raising programmes (which might include an element of direct marketing). It is intended that non-resident members’ contact details will be made available to other resident and non-resident members of the College, recognised non-resident members’ societies (e.g. Sidney Sussex Society) in the UK and overseas, to sports and other clubs associated with the College, and to agents contracted by the College for particular alumni-related activities. The Development Office will seek individuals’ consent to disclosure of their contact details. If an individual has an objection to other aspects of the processing of their data for administrative or fund raising purposes, then written notice should be given to the Development Officer.

**Data Area Contact:** Membership and Events Officer

**Computer Databases.** Certain of the files referred to above are maintained in electronic databases as well as, or instead of, paper files. Access to such databases is restricted in the same manner as access to paper files in the relevant Data Area. In addition, however, the Computer Officer may have day-to-day access to the electronic databases for the purposes of administering and maintaining the same. These computer databases include, but are not limited to, the following: APT solutions (Development Office), Sage (College Office), FoxPro (Admissions), IP database (Computer Office) and Heritage Library Management (Library).

**Data Area Contact:** Computer Officer

**SECURITY OF PERSONAL DATA HELD ON COMPUTERS**

All reasonable steps should be taken to ensure that personal data held on computers is secure. The following steps are suggested:

- access to computer files should be restricted using privilege levels and passwords.
- regular password changes should be enforced and the number of attempted logins limited.
• equipment should be sited in a secure location where access can be restricted to authorised personnel. Members of the public should not be able to view terminal screens.
• terminals should not be left unattended and should be logged off at the end of the session.
• redundant data should be wiped or overwritten.
• appropriate back up and storage should be observed.
• removable disks should be locked up after use.
• for large amounts of sensitive data, it might be necessary to keep a copy in a fireproof safe at a separate location.
• network systems can be accessed by experienced persons. Whenever possible, personal data should be encrypted to prevent unauthorised access.
• computer printout containing personal information should be shredded before disposal; it should not be used as scrap paper.

CCTV
The College operates a number of CCTV cameras in order to assist with security for members of the College Community and in respect of College property. If an individual has any queries regarding the operation of the CCTV system, they should contact the Domus Bursar. The tapes are held in secure conditions for 13 days, and on the 14th day they are erased. If anyone wishes to access any personal data about themselves on the CCTV system within 13 days of the occurrence, they should complete and return a Subject Access Request form (with the requisite £10 fee) with as much information as possible to enable the data to be located (including, if possible, details of the relevant camera, date and time).

EMAIL
It is permissible and appropriate for the College to keep records of internal communications which are relevant to an individual’s ongoing relationship with the College, whether as a Fellow, member of staff or student, including information concerning performance and conduct issues, provided such records comply with the Data Protection principles. It is recognised that email is used for such communications and that such emails should form part of the College's records. It goes beyond the scope of this policy document to address the appropriate use of email in the proper functioning of the College, and the limitations and legal implications with this mode of communication. However, all members of the College need to be aware that:
• DPA98 Act applies to emails which contain personal data about individuals which are sent or received by members of the College (other than for their own private purposes as opposed to College purposes);
• subject to certain exceptions, individual data subjects will be entitled to make a data Subject Access Request and have access to emails which contain personal data concerning them, provided that the individual data subject can provide sufficient information for the College to locate the personal data in the emails; and
• the legislation applies to all emails from and to members of the College which are sent and received for College purposes, whether or not the emails are sent through the College email system or on an individual’s own email account.

DISCLOSURE OUTSIDE OF THE EEA
The College may, from time to time, desire to transfer personal data to countries or territories outside of the EEA in accordance with purposes made known to individual data subjects. For example, the names and contact details at the College of members of staff on a website may constitute a transfer of personal data worldwide. Accordingly, the consent form signifies an individual’s consent to the inclusion of such data on an authorised College website. If an individual wishes to raise an objection to this disclosure then written notice should be given to the Data Protection Officer. Other personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the EEA to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects.

CLUBS AND SOCIETIES
It is the responsibility of each Club or Society to ensure that any personal data held or processed on their members is carried out in accordance with the Data Protection Act. The College accepts no responsibility in this regard.

Senior Tutor
November 2010