

**Girton College**  
**Data Protection Policy**  
February 2010

**Contents:**

1. Purpose
2. Scope
3. Responsibilities under the Act
4. Notification to the Information Commissioner
5. Data Protection Principles
6. Processing Sensitive Information
7. Subject Consent
8. Data Security and Disclosure
9. Right of Access to Data
10. Disclosure outside the European Economic Area (EEA)
11. Data Areas
12. Policy Review

**1. Purpose**

Girton College processes information about its employees, applicants, students, alumni and other individuals for purposes such as the administration of the admissions process, the effective provision of academic and welfare services and to operate the payroll. This policy aims to ensure that in so doing the College complies with the Data Protection Act 1998 ("the Act") and that personal information is collected and used fairly, stored safely and not disclosed to any unauthorised person.

**2. Scope**

This policy applies to all staff and Fellows of the College where they are acting in the course of their duties as its employees and to students and other members of the College where they are acting on its behalf or under its instruction. It applies to all personal data processed in the course of the activities described above, regardless of format (paper, digital or audio-visual) and location (processed on College premises or elsewhere). Personal data are any data relating to a living, identifiable individual or to an individual who may be identifiable from those data if put together with other data. Further guidance and procedures on data collection, storage and processing can be found on the College's website.

**3. Responsibilities under the Act****Data Controller**

The College (i.e. The Mistress, Fellows and Scholars of Girton College) is the Data Controller.

**Data Protection Officer**

The College Data Protection Officer is the Bursar.

**Data Protection Co-ordinator**

All queries about the College policy and all requests for access to personal data should be addressed to the Data Protection Co-ordinator (see "Right to Access Personal Data" below).

**Data processors**

All members of the College who process personal data in any form are data processors and must ensure they comply with the requirements of the Act and with the College's data protection policy (including any additional data protection procedures and guidelines that may be issued by the College from time to time).

In particular, no member of the College may, without the prior written authorisation of the Data Protection Officer:

- 1) develop a new computer system for processing personal data;
- 2) use an existing computer system to process personal data for a new purpose;
- 3) create a new paper filing system containing personal data;
- 4) use an existing paper filing system containing personal data for a new purpose.

A breach of the Act and/or the College's data protection policy may result in disciplinary proceedings.

### **Admissions 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 Tutor or Admissions Office in the case of candidates or the Senior Tutor or Tutorial Office in the case of Students.

Students must comply with the College's Computing Regulations (available on the College's website).

Student organisations such as the JCR, MCR and College societies must ensure they manage personal data in accordance with this policy.

#### **4. 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. Individual data subjects can obtain full details of the College's data protection notification with the Information Commissioner from the College Data Protection Co-ordinator or from the Information Commissioner's website (<http://www.ico.gov.uk/ESDWebPages/search.asp>).

#### **5. Data Protection Principles**

The College, as a Data Controller, must comply with the Data Protection Principles, which are set out in the Act. In summary these state that personal data shall:

- 1) Be processed fairly and lawfully and shall not be processed unless certain conditions are met.
- 2) Be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes.
- 3) Be adequate, relevant and not excessive for those purposes.
- 4) Be accurate and kept up to date.
- 5) Not be kept for longer than is necessary for those purposes.
- 6) Be processed in accordance with the data subject's rights under the 1998 Act.
- 7) Be the subject of appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction.
- 8) Not be transferred to a country outside the European Economic Area, unless that country or territory has equivalent levels of protection for personal data.

## **6. Processing Sensitive Information**

Sometimes it is necessary to process information about a person's criminal convictions, race, gender, health and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or equal opportunities policy. The College may also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes or disabilities. The College will only use the information in the protection of the health and safety of the individual, but will need consent to process, for example in the event of a medical emergency. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the College to do this.

Full guidance on the creation and processing of data for members of the College is available in the College website data protection pages.

## **7. Subject Consent**

In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974. The College has a duty of care to all staff and students and must therefore make sure that all employees and those who use the College's facilities do not pose a threat or danger to other users. Therefore, all prospective staff and students will be asked to consent to their data being processed when an offer of employment or a course place is made. A refusal to sign such a form may result in the offer being withdrawn.

## **8. Data Security and Disclosure**

All members of the College are responsible for ensuring that:

- Any personal data they hold is classified and managed in accordance with the University's Information Security Policy (<http://www.admin.cam.ac.uk/reporter/2001-02/weekly/5895/8.html>).
- Personal data is not disclosed 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 is kept securely. Further guidance on keeping data securely can be found on the College's records management website pages.

## **9. Right to Access Personal Data**

Individuals have the right under the Act to access any personal information that is being held about them by the College and to request the correction of such information if it is incorrect. An individual who wishes to exercise his/her right of access is asked to complete the College "Access to Personal Data" form available from the College website or in hard copy directly from the Data Protection Co-ordinator.

Any inaccuracies in data disclosed in this way should be communicated immediately to the Data Protection Co-ordinator 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 Data Protection Act 1998) on each occasion that access is requested and this fee should accompany the "Access to Personal Data" form. In accordance with the Act, the College reserves the right to refuse repeated requests where a reasonable period has not elapsed between requests.

The College will respond to the request for access to personal data within 40 calendar days (including bank holidays and weekends) of the request or payment of the fee, whichever is the later.

#### **10. Disclosure outside of the EEA**

The College may, from time to time, wish to transfer personal data to countries or territories outside of the European Economic Area (EEA) in accordance with purposes made known to individual data subjects. For example, the names and contact details of members of College staff on a website may constitute a transfer of personal data worldwide. The College will always seek the express consent of data subjects before posting such personal information on the worldwide section of the College website.

Other personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures are 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.

#### **11. "Data Areas"**

##### **CCTV**

The College operates a number of CCTV cameras in order to ensure the security of members of the College and its property. Queries regarding the operation of the CCTV system should be directed to the Head Porter or the Warden of Wolfson Court. If you wish to access any personal data about you on the CCTV system, you are asked to complete and return an "Access to Personal Data" 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). Please bear in mind that CCTV images are only kept for 7-10 days and are then overwritten. It is therefore important to ask for access to CCTV images as soon as possible.

##### **Photography and the use of images**

All employees, students and visitors to the College should be aware that the image of **a clearly identifiable person** comes within the Data Protection Act's definition of 'personal data'. The image may appear in (and is not exclusive) to the following formats:

- Photographs
- Videos
- Paper publications
- The internet
- CCTV
- Mobile phones

In order to comply with the Data Protection Act, **explicit consent for any clearly identifiable person will be obtained** prior to taking the image and/or before any publication of the image.

All images will be stored securely and used only for their intended purposes. At College events, every effort will be taken to obtain consent from individuals and groups before a photograph is taken or published, stating the purpose for taking the

photograph and its intended use. Images will not be used on the website without prior consent from the person. Guidance on the use of images and Photograph consent forms are available on the College website.

All members of College and visitors should note that the use of webcams in College or the College grounds is not permitted without prior permission from the Data Protection Officer and Council. In addition, care must be taken when taking photographs in the vicinity of the College's student accommodation.

### **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 form part of the College's records. All members of the College need to be aware that:

- the 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.

### **College Archives**

After a member of staff or Fellow leaves the College, his or her file(s) will be transferred to semi-current storage and from there to the College's archives once it is no longer required for administrative purposes. The personal information contained in these files form part of the archives of the College, and will be retained indefinitely for consultation by third parties for statistical, historical or biographical research purposes. Access to the archives both by College employees and external researchers will be managed in accordance with the Act.

### **Alumni Relations and Development**

Manual and computer based files are maintained in respect of some current and former Fellows, alumni, and other current, past and potential donors to the College. All files are to be kept in either the locked Development Office or the locked Roll Office and access to the computer database is password protected. Development Office staff and Roll Office staff may consult the manual and computer based files on a day to day basis, but requests by others to view these files must be authorised by the Development Director or the Registrar of the Roll.

Data will be used by the College for a full range of alumni activities, including the sending of College publications, promotion of benefits and services available to alumni (including those being made available by external organisations), notification of alumni activities and fund raising programmes (which might include an element of direct marketing).

With explicit permission from the individual, the contact details of Alumni can be made available to other current and old members of the College, recognised alumni societies 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' explicit consent to the disclosure of their contact details. If an individual has an objection to other aspects of the processing of their data for alumni or fund raising purposes, then written notice should be given to the Development Director.

## **12. Policy Review**

This policy was approved by Council in February 2010, and replaces the existing Data Protection Policy. It will be reviewed again in February 2012.