JESUS COLLEGE
CAMBRIDGE

Identification and Handling of Confidential Information

This policy is aimed at Fellows, Staff and Students using College information.

Policy Abstract: Some information created by the College is sensitive and should be kept confidential. In the case of personal data this is a legal requirement under the Data Protection Act 1998 and the College could now face substantial financial penalties for not taking all reasonable steps to ensure confidentiality.

In other cases the College's interests could be damaged by disclosure. This policy sets out the College's requirements for the secure handling of confidential information.

Classes of information to be treated as confidential:

- Personal data about identifiable living individuals.
- Reserved minutes of official College bodies.
- Information that may be of commercial value to the College.
- Legal or professional advice received by the College.
- Information about security measures and the location of critical services.
- Information provided in confidence to the College either in writing or orally.

Working with confidential information

Confidential information should be securely marked as such and distributed appropriately. Serious consideration should be given to who receives the confidential information and what the justification is for its distribution in the first place.

Confidential information should not be left unattended and unlocked.

Computers should be locked when unattended to prevent unauthorised access to College systems.

Computer system passwords should not be disclosed to anyone.

Photocopiers and shared printers should be used with care. Do not store scanned documents in the shared copier folders or leave papers in copiers or printers.

Avoid working on sensitive information in public places where you can be easily overlooked or where there could be a risk of accidental loss or theft.
Do not discuss the contents of confidential documents with colleagues in an open environment.

Information should not be taken out of College without the consent of the Head of Department, or if electronically, in consultation with the IT Department.

Care should be taken with any information taken off the premises and its loss reported promptly.

Any person wishing to discuss confidential or personal matters should be entitled to do so in a private place.

Any breach or suspected breach of confidentiality should be reported to the Departmental Manager or the Bursar.

Requests for information

Do not send confidential information to anybody not authorised to see it.

If the person requesting the information claims that they have a right to see it, then proper identification and verification should be obtained before disclosure, even if that person is from an official body such as the police.

All non-routine requests for information should be made formally and in writing.
Any request for personal information should be accompanied by the person's full name and address and verification of that person's identity.

If the personal information requested is about a third party then the applicant should supply written identification and verification of their right to see the information.

If the subject of the information is believed to be deceased but could reasonably still be alive then proof that the person has died should be obtained.

Personal files may also contain information about a third party, for example family and friends and other people interacting with that person. These should not be disclosed without that third party's consent.

The public has a right to ask the College for information under the Freedom of Information Act, but exemptions may apply to confidential material. Do not respond to Freedom of Information Act requests - pass these on to the Records and Information Manager.

Sending confidential information

- Always use a sealed envelope or package.
- Mark as "confidential addressee only".
- Avoid committing confidential information to e-mail.
- Do not use e-mail or other forms of electronic communications to express opinions about people or about confidential matters.
- Documents sent externally or posted on the College website or JNET should use the pdf format to avoid the possibility of documents being tampered with.
- If you need to send files to Archives always ask the Porters to store them securely in the "confidential" box in the Lodge and inform Archives staff so that they can collect them.

Disposing of confidential information

- Never commit anything that may be sensitive to the ordinary waste bin or green box.
- Use the secure shredding bins for personal or other confidential information. The bins are kept locked and the paper from them is shredded on site and then recycled.
- Arrangements to send large amounts of paper for confidential shredding should be made directly with the Records and Information Manager and not with the Housekeeping Department.
- Do not dispose of any electronic media without the IT Department's consent and advice where appropriate.

A retention schedule for all College data can be found on JNet, published under the IT Department section. This schedule is reviewed regularly.

Appendix A

Definition of Confidential Information

1. Personal information relating to fellows, students, staff, old members, donors, tenants, visitors, B&B and conference guests or any individual with whom the College has dealings.

This covers all records of identifiable living people, so could include paper and computer files, unstructured information such as e-mails, photographs, CCTV and other moving images and even voicemail.

The College would be liable to censure and possibly a heavy fine if this information were to be misused to the damage and distress of the individual concerned. This is most likely to occur if the information is lost, stolen or seen by people with no good reason for seeing it. All requests for personal information should be treated with care and according to the above policy to avoid inadvertent disclosure.

In some cases it is correct to disclose personal information. Individuals have subject access rights to see the information that we hold about them. Data Protection legislation does not apply to people who are no longer living, nor to people who cannot be identified from it. Organisations such as the police have certain rights to obtain personal information in the course of their duties.

If the person does have a demonstrable right to see personal information then it is important that the College can locate and collate this information in good time and present it to them in a secure and professional manner.

2. Reserved Minutes of Official College bodies may contain personal information. They may refer to sensitive matters whose disclosure would damage the College's reputation or commercial interests. It is also important to retain absolute confidentiality to protect the record of the College's business and decision making,

guarantee rights to free speech of participants and to ensure that advice contained in them is given honestly and frankly.

Examples include but are not limited to minutes and associated papers of Council, Society, Staff Committee, Buildings Committee and working parties. Also includes papers of College groups set up to oversee important projects.

3. Information that may be of commercial value to the College. Disclosure may affect the commercial competitiveness of the College and put it at a disadvantage against organisations offering similar services. Examples could include information relating to conferences, large building projects, contacts with potential donors, alumni relations, events and meetings, procurements and some salary information.

4. Legal or professional advice received by the College. It is in the College's interests that the advisors that we employ can speak freely and give honest opinions. Advice given in this category might include solicitors, property agents, architects, auditors, investment advisors, accountancy services, tenders, contracts and formal contact with contractors and other providers of specialist services.

5. Information about security measures and the location of critical services. Confidentiality should be maintained to mitigate risk to College property and individuals on the premises. Examples may include exact CCTV camera locations, insurance details, details of deliveries and site meetings for building contracts. Also includes precise details of wine, silver and works of art, books and manuscripts stored by the College and their exact location, along with supply points for water, electricity, gas, oil and the IT and telephone networks

6. Information provided in confidence to the College either in writing or orally. The College needs to obtain correct and honest information in order to make accurate operational decisions. This information may not be in a structured form and may well be delivered orally. All types of information will be treated carefully so that people supplying the information understand that their privacy will be respected. Examples might include information about individual financial circumstances, information provided to directors of studies by students and information provided to managers and the HR Manager by staff.

Appendix B

Privacy of users and investigations of accounts

Although it will take all reasonable measures to respect the privacy of system users, the College can accept no responsibility for maintaining confidentiality of personal or other information not related to its business held on its systems. Users are advised to keep such information to an absolute minimum.

Where the College has reasonable grounds to suspect that activity contrary to its regulations and detrimental to its interests, is taking place, then it may authorise the investigation of users' accounts on its IT systems. Where routine monitoring of people

visiting or using the College facilities or systems is taking place then the College will keep subjects informed that this is happening.

The College routinely monitors and collects information on access to its premises and the use of many of its IT systems. For example data is collected via the College CCTV system to help prevent theft and ensure the security of the College community and buildings, through third party companies for monitoring possible abuse of the mobile phone system, and through its network monitoring systems to catch any unusual network activity.

Appendix C

Legislation that may affect this policy The Data Protection Act 1998
Privacy and Electronic Communications (EC Directive) Regulations 2003
The Freedom of Information Act 2000
The Environmental Information Regulations 2004