GREEN TEMPLETON COLLEGE | OXFORD

Data Protection Policy

1. Introduction

Like all educational establishments, Green Templeton College holds and processes information about its students, fellows, employees, alumni and other individuals for various operational and legal purposes.

The College is compliant with the requirements of the Data Protection Act 1998 (DPA) which came into force on 1 March 2000 and protects individuals against the possible misuse of information held by others about them. Information that is already in the public domain is exempt from the Act.

2. Definitions

Personal data
Personal data means data relating to a living individual who can be identified from that information, or from that and other information in the possession of the Data Controller. This data may be held on paper or electronically.

Sensitive personal data
Sensitive personal data means data relating to race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life or criminal activities.

Processing data
Obtaining, recording or holding the data or carrying out any activity on that data including:

- Organisation, adaptation or alteration of the data.
- Retrieval, consultation or use of the data.
- Disclosure of the data by transmission, dissemination or otherwise making available.
- Alignment, combination, blocking, erasure or destruction of the data.

3. Notification to the Data Protection Commissioner

The College has an obligation as a Data Controller to notify the Data Protection Commissioner of the purposes for which it holds and processes personal data. A summary of the main categories of data that the College may hold and process is in Appendix A.

4. Principles

The DPA established eight principles, which require personal data to:

I. Be processed fairly and lawfully.
II. Be obtained for lawful and specific purposes.
III. Be adequate, relevant and not excessive.
IV. Be accurate and kept up-to-date.
V. Not be kept longer than necessary.
VI. Be processed in accordance with the rights of data subjects.
VII. Be kept under appropriate technical and organisational security measures.
VIII. Not be transferred outside the European Economic Area (EEA) unless that country has equivalent levels of protection for personal data.

5. Fair and lawful processing

In order to comply with the first principle, the College must ensure that at least one of the following conditions are met:

- An individual has given their consent to the processing.
- The processing is necessary for the performance of a contract with the individual.
- Processing is required under a legal obligation.
- Processing is necessary to protect the interests of an individual.
- Processing is necessary to carry out public functions.
- Processing is necessary in order to pursue the legitimate interests of the Data Controller or third parties (unless it could prejudice the interests of the individual).

Additional restrictions are in place for processing sensitive personal data and explicit consent from individuals will normally be required.

6. Consent and disclosure

When a student signs their College contract, they permit the College to hold and process particular types of data about them (as outlined in Appendix A). Individuals can raise objections to the intended processing of the data, which will be considered by the Data Protection Officer. However, the College reserves the right to process data for effective administration purposes. Students should also refer to their University contract which includes a note on data protection.

The College undertakes to ensure appropriate technical and organisational measures are in place to prevent the unauthorised disclosure of personal data and to protect against its accidental loss or destruction. Further details are provided in the College's Information Security Policy.

Personal data is not normally provided to parties external to the collegiate University. Special arrangements apply to the exchange of data between the University and the colleges. The College may disclose data to law enforcement authorities if there are concerns over criminal activity.

7. CCTV and door entry systems

The College operates a number of CCTV cameras and a door entry system in order to provide security for members of the College community and the College properties. Access to the data from these systems is usually restricted to the Bursar, Domestic Bursar, Accommodation Officer and Lodge Staff. IT staff access the systems for routine management and maintenance and are also authorized to assist with the retrieval of data.

8. Responsibilities

All members of the College should be aware of the requirements of this data protection legislation and of their individual responsibilities under it. The College insists that its members are careful not to disclose personal data to any unauthorised person. Further guidance for employees, or other individuals, who have access to personal data is in Appendix B.

The College recognises that any failure to comply with the data protection legislation may render the College, or in certain circumstances an individual responsible, liable to prosecution as well as giving rise to civil liabilities. Any breach will be taken seriously and may result in disciplinary action.

9. Access to personal data

Individuals have the right to access any personal data that is being held about them and to request the correction of this data where it is incorrect.

To exercise this right, individuals are asked to complete the *Access to Personal Data* form in Appendix C and return it to the College Data Protection Officer together with an administration fee of £10 and proof of identification.

The College will respond to requests for access to personal data within 40 days of receipt unless there is a good reason for delay. Any delay will be explained to the individual making the request. Further details on the process can be found in Appendix C.

10. Data Protection Officer

The College Data Protection Officer is the Head of Library and Information Services. Any questions or concerns about the interpretation or operation of this policy should be addressed to Kirsty Taylor (kirsty.taylor@gtc.ox.ac.uk). Requests for access to, or corrections of personal data, should also be addressed to the Data Protection Officer.

11. Further information

A guide to the University policy and the responsibilities of individuals working in the University is at: http://www.admin.ox.ac.uk/councilsec/dp/policy.shtml

Further information and advice on data protection is available at: http://ico.org.uk/

Appendix A: Summary of Data

The following is a summary of the main categories of data that Green Templeton College holds and processes, the main purposes for holding/processing the data, the possible disclosures of the data and the likely sources of such data. Individuals can obtain full details of the College's registration with the Data Protection Commissioner from http://ico.org.uk/.

Data	Personal details; academic record; qualifications and skills; student record; student financial record.
Main Purposes	To assess applications from candidates for admission and assist in the admissions process; accommodation issues; to process proper and up-to-date records of academic progress; to administer and collect fees and charges; legal issues and obligations (e.g. Health & Safety record); communications/mailings; references; undertaking research and fundraising; alumni activities; event management.
Main Sources & Disclosures	Applications forms; event booking forms; family; local authority (and other governmental bodies); examination results; scholarships; Student Loans Company; University of Oxford; College staff and committees; other Oxford Colleges; other Universities; schools; examination boards; other educational institutions; employers and potential employers; legal representatives; law enforcement authorities, admissions officers.

Data	Medical information
Main Purposes	Provision of healthcare; welfare; dietary requirements; accommodation issues.
Main Sources & Disclosures	Application form; Data subject; Family; College Nurse; Senior Tutor; other College staff; University of Oxford; General Practitioners; other medical practitioners.

Data	Ethnic origin
Main Purposes	Equal opportunities monitoring; dietary requirements.
Main Sources & Disclosures	Application form; research and statistical purposes; College staff.

Data	Criminal records
Main Purposes	Disciplinary matters; legal obligations.
Main Sources & Disclosures	Application forms; Police (& other authorities); legal representatives; court service; University of Oxford; College staff; other colleges.

Data	CCTV images and door entry records
Main Purposes	Security; prevention and detection of crime; health and safety; disciplinary purposes.
Main Sources & Disclosures	CCTV system; Net2 door entry system; college staff; University security; Police (& other authorities).

Appendix B: Responsibilities of Data Users

All College members who have hold or have access to personal data in any form must comply with the requirements of the Data Protection Act 1998 and with this College policy. A breach may lead to disciplinary proceedings.

Data users must ensure that:

- Any personal data they hold is kept securely. If the personal data is kept in paper records, these must be kept in a locked filing cabinet, drawer or office whenever unattended. If the data is electronic, it should be stored on one of the College network drives, which are secured by IT. PCs and laptops used to access the data must be password-protected and passwords must not be shared with anyone. Personal data must not be stored on laptops or memory sticks, unless these are fully encrypted. Memory sticks must provide hardware based encryption.
- Personal data is not disclosed either orally or in writing, accidental or otherwise, to any unauthorised third party.
- Personal data is kept and used for the purpose for which it was given.
- Personal data is not kept for longer than necessary. Routine housekeeping schedules will need to be followed for the disposal of data.
- Documents containing personal data are disposed of securely. Paper copies should be deposited in the shredding bins situated around College. Electronic copies should be deleted from the network drive and from any other storage media (e.g. memory sticks) when no longer required.
- Any loss or potential compromise of personal data is reported to the Data Protection Officer immediately.
- They provide any personal data promptly when requested by the Data Protection Officer in order to satisfy a subject access request.

Appendix C: Access to Personal Data

If you wish to make a 'data subject access request' pursuant to the Data Protection 1998, please do the following:

1. Fill in the relevant sections of the forms on pages 7 and 8.
2. Provide a **copy** of proof of identification.

   Accepted forms of identification include: a driving licence, a birth certificate or pages from a passport showing your name, passport number and photograph.

   Please note that, if you're requesting CCTV images, we will ask you to supply a photograph of yourself to ensure only your images are disclosed.

   The College requires proof of identification because it has a legal duty to ensure that personal data is only disclosed to those entitled to have access.
3. Arrange to pay the administration fee online or fill in your credit card details (see page 3 for details).
4. Return this form to the College's Data Protection Officer at:

   Kirsty Taylor
   Head of Library and Information Services
   Green Templeton College
   Woodstock Road
   Oxford
   OX2 6HG
5. The Data Protection Officer will send an acknowledgement on receipt of your request, proof of identification and fee. The College will respond to your request within 40 days unless there is a good reason for delay. In such cases, the reason for delay will be communicated to the requestor.

The College reserves the right to refuse vexatious or repeated requests unreasonably often. The College may be unable to provide information that contains data about or identifies third parties.

N.B. The data gathered by this form will be used to process your request for personal data under the Data Protection Act 1998. It will be held by Green Templeton College's Data Protection Officer and may be transferred to other parts of GTC in order to respond to your request. The data will be held for six years from the date we respond to your request. If your request forms part of an ongoing case we will keep the data for as long as necessary.

GREEN TEMPLETON COLLEGE | OXFORD

Access to Personal Data Request Form

I would like copies of personal data held about me, in so far as the information is governed by the Data Protection Act 1998, in the categories set out in this form:

Family name:	**First name(s):**
Date of birth:	**Student number:** *(if applicable)*
Address for data to be sent to:	

Type of data	**Please tick as appropriate**
Student records: admissions	
Student records: disciplinary	
Student records: academic staff records	
Computing records	
Library records	
Financial records	
Accommodation records	
Medical records	
Personnel records	
Door entry records	
CCTV *(please provide dates & times below)*	
Other *(please specify)*	

Further details *(dates & times for CCTV etc.)*
Signed:
Date:

Payment Details

Payment of the £10 administration fee can be made direct to our bank:

Barclays Bank plc. Oxford Corporate Group, PO Box 333, Oxford OX1 3DD
Sort code 20 65 18
Account Number 80883018
Bank Swift Number BARCGB22
Branch Swift Number BARCGB2108P
IBAN Number GB45 BARC 2065 1880 8830 18

PLEASE QUOTE '**DATA PROTECTION'** WHEN MAKING A PAYMENT.

Alternatively, you can by pay by credit or debit card by completing the details below. Do not email the form back to us as we cannot guarantee online security.

Name of cardholder	
Card Type (Visa, MasterCard etc.)	
Card Number	
Valid From (month/year)	
Expiry Date (month/year)	
Security Code (last 3 digits)	
Please charge my credit/debit card with £10	
Signature of cardholder	

College use only

Date form received	
ID?	
Fee paid?	
Date response sent	