OXFORD TUTORIAL COLLEGE

Data Protection Policy

Revised August 2017
To be reviewed May 2018

Section 1 - Policy Statement

Oxford Tutorial College is committed to a policy of protecting the rights and privacy of individuals (this includes students, staff and others) in accordance with the Data Protection Act. The College needs to process certain information about its staff, students and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programs of study, to record progress, to agree awards and to collect fees). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all staff and students of the College. Any breach of the Data Protection Act 1998 or the College Data Protection Policy is considered to be an offence and in that event, Oxford Tutorial College disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the College, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that departments/sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

Section 2 - Definitions (Data Protection Act 1998)

Personal Data	Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, ID number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual
Sensitive Data	Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing
Data Controller	Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed
Data Subject	Any living individual who is the subject of personal data held by an organisation
Processing	Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data; accessing, altering, adding to, merging, deleting data; retrieval, consultation or use of data; disclosure of or otherwise making data available
Third Party	Any individual/organisation other than the data subject, the data controller (College) or its agents
Relevant Filing System	Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be

	readily extracted.

Section 3 - Data Protection Principles

All processing of personal data must be done in accordance with the eight protection principles:

1. **Personal data shall be processed fairly and lawfully.** Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, of any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

2. **Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.** Data obtained for specified purposes must not be used for a purpose that differs from those.

3. **Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.** Information which is not strictly necessary for the purpose for which it is obtained should not be collected. If data are given or obtained which are excessive for the purpose, they should be immediately deleted or destroyed.

4. **Personal data shall be accurate and, where necessary, kept up to date.** Data which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the College are accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein are accurate. Individuals should notify the College of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the College to ensure that any notification regarding change of circumstances is noted and acted upon.

5. **Personal data shall be kept only for as long as necessary.** (See section 10 on Retention and Disposal of Data)

6. **Personal data shall be processed in accordance with the rights of data subjects.** (See section 5 on Data Subject Rights)

7. **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.** (See section 7 on Security of Data)

8. **Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.** Data must not be transferred outside of the European Economic Area (EEA) (Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece,

Hungary, Iceland, Republic of Ireland, Italy, Liechtenstein, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom) - without the explicit consent of the individual.

Commented [JE1]: This may be interesting for safeguarding…

Section 4 - Responsibilities under the Data Protection Act

- The College as a body corporate is the data controller
- The senior officer responsible for the College's compliance with the Data Protection Act is the Technical Manager
- The Senior Management team and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within the College
- Compliance with data protection legislation is the responsibility of all members of the College who process personal information
- Members of the College are responsible for ensuring that any personal data supplied to the College are accurate and up-to-date

Section 5 - Data Subject Rights

Data Subjects have the following rights regarding data processing and the data that are recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for the purposes of direct marketing
- To be informed about the mechanics of any automated decision taking process that will significantly affect them
- Not to have significant decisions that will affect them taken solely by automated process
- To sue for compensation if they suffer damage by any contravention of the Act
- To take action to rectify, block, erase or destroy inaccurate data
- To request the Information Commissioner to assess whether any provision of the Act has been contravened

Section 6 – Consent

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The College understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and sensitive data is obtained routinely by the College (eg when a student signs a registration form or when a new member of staff signs a contract of employment). Any College forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data are to be published on the Internet as such data can be accessed from all over the globe. Therefore, not gaining consent could contravene the eighth data protection principle.
If an individual does not consent to certain types of processing (eg direct marketing), appropriate action must be taken to ensure that the processing does not take place.

Section 7 - Security of Data

All staff are responsible for ensuring that any personal data on others which they hold are kept securely and that they are not disclosed to any unauthorised third party (see Section 9 on Disclosure of Data for more detail).
All personal data should be accessible only to those who need to use them. You should form a judgment based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- in a lockable room with controlled access, or
- in a locked drawer or filing cabinet, or
- if computerised, password protected, or
- kept on disks (such as USB flash drives) which are themselves kept securely

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff and students who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and students should take particular care when processing personal data at home or in other locations outside of the College buildings.

Section 8 - Rights of Access to Data

Members of the College have the right to access any personal data which are held by the College in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the College about that person.

Section 9 - Disclosure of Data

The College must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and students should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of College business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the College concerned.

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- To safeguard national security*
- Prevention or detection of crime including the apprehension or prosecution of offenders*
- Assessment or collection of tax duty*
- Discharge of regulatory functions (includes health, safety and welfare of persons at work)*
- To prevent serious harm to a third party
- To protect the vital interests of the individual; this refers to life and death situations

*** Such requests must be supported by the appropriate paperwork**

When members of staff receive enquiries as to whether a named individual is a member of the College, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the College may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

Section 10 - Retention and Disposal of Data

The College discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and students. However, once a member of staff or student has left the institution, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

Students
In general, electronic student records containing information about individual students are kept indefinitely and information would typically include name and address on entry and completion, programs taken, examination results, awards obtained.

Staff
In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by the Personnel Department for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc will be retained for the statutory time period (between 3 and 6 years).

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. Personnel may keep a record of names of individuals that have applied for, been short-listed or interviewed for posts indefinitely. This is to aid the management of the recruitment process.

Disposal of Records
Personal data must be disposed of in a way that protects the rights and privacy of data subjects (eg, shredding, disposal as confidential waste, secure electronic deletion).

Section 11 - Direct Marketing

Any department or section that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (eg an opt-out box on a form).

Section 12 - Use of CCTV

For reasons of personal security and to protect College premises and the property of staff and students, a close circuit television camera is in operation at the main entrance to the College building at 12 King Edward Street and over the entrance to Cambridge Terrace. The presence of these camera may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:

- Any monitoring will be carried out only by a limited number of specified staff
- The recordings will be accessed only by the Senior Management Team, Technical Manager and Receptionist
- Personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete
- Staff involved in monitoring will maintain confidentiality in respect of personal data

For further guidance or advice on the Data Protection Act, please contact the Technical Manager: Sukh Sanghera, email: Sukh.Sanghera@oxfordtutorialcollege.com or telephone: 01865 793333.