Regent's Park College

Data Protection Policy

The Data Protection Act 1998

The Data Protection Act (DPA) gives individuals the right to know what information is held about them, and provides a framework to ensure that personal information is handled properly.
The Act came into force on 1 March 2000 and covers personal data held on computer and in manual files. It also imposes restrictions on the transfer of data outside the European Economic Area, which has particular implications for placing material on the web. The College must comply with eight data protection principles, which make sure that personal information is:

1. fairly and lawfully processed;

2. processed for limited purposes;

3. adequate, relevant and not excessive;

4. accurate and up to date;

5. not kept for longer than is necessary;

6. processed in line with the rights of individuals;

7. secure; and

8. not transferred to other countries without adequate protection.

Anyone holding information relating to individuals in the course of their work must therefore consider:

- whether the information they hold is subject to the provisions of the new Act;
- whether the arrangements they have in place satisfy the requirements of the Act, for example in relation to security of the data concerned; and
- whilst data access requests are handled centrally by the College's Data Protection Officer, what procedures are in place to facilitate a prompt response to requests for data.

The Information Commissioner's Office is the UK's independent authority set up to promote access to official information and to protect personal information. Every organisation that processes (i.e. holds and uses) personal information must be registered with the Information Commissioner's Office (ICO), unless they are exempt. The College's registration number is **Z8586816**.

For more detailed guidance

The legislation is complex and more detailed guidance is available on the Information Commissioner's website.

Regent's Park College

Data Protection Policy

College Policy on Data Protection

The primary purpose of current data protection legislation is to protect individuals against possible misuse of information about them held by others. It is the policy of the College to ensure that all members of the College and its staff are aware of the requirements of data protection legislation under their individual responsibilities in this connection.

The Act covers personal data, whether held on computer or in certain manual files.

The College is obliged to abide by the data protection principles embodied in the Act. These principles require that personal data shall:

- be processed fairly and lawfully;
- be held only for specified purposes and not used or disclosed in any way incompatible with those purposes;
- be adequate, relevant and not excessive;
- be accurate and kept up-to-date;
- not be kept for longer than necessary for the particular purpose;
- be processed in accordance with data subject's rights;
- be kept secure;
- not be transferred outside the European Economic Area unless the recipient country ensures an adequate level of protection.

Definitions and guidance on what constitutes fair and lawful processing (principle 1) may be found below.

The Act provides individuals with rights in connection with personal data held about them. It provides individuals with the right to access data concerning themselves (subject to the rights of third parties). It also includes the right to seek compensation through the courts for damages and distress suffered by reason of inaccuracy or the unauthorised destruction or wrongful disclosure of data. Information on how to make a request for access to personal data under the Act may be obtained from the Principal's PA.

Under the terms of the Act, processing of data includes any activity to do with the data involved. All staff or other individuals who have access to, or who use, personal data, have a responsibility to exercise care in the treatment of that data and to ensure that such information is not disclosed to any unauthorised person. Examples of data include address lists and contact details as well as individual files. Any processing of such information must be done in accordance with the principles outlined above. In order to comply with the first principle (fair and lawful processing), at least one of the following conditions must be met:

- the individual has given his or her 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 vital interests of the individual;

- processing is necessary to carry out public functions;
- processing is necessary in order to pursue the legitimate interests of the controller or third parties (unless it could prejudice the interests of the individual).

In the case of sensitive personal data, which includes information about racial or ethnic origins; political beliefs; religious or other beliefs; trade union membership; health; sex life; criminal allegations, proceedings or convictions, there are additional restrictions and explicit consent will normally be required.

In relation to security (Principle 7), the Data Controller (the College) must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data and sets out specific considerations for ensuring security. Staff and other individuals should be aware that guidelines and regulations relating to the security of manual filing systems and the preservation of secure passwords for access to relevant data held on computer should be strictly observed.

Staff should also note that personal data should not normally be provided to parties external to the College. Special arrangements apply to the exchange of data between the University and the colleges. For further guidance on this, please contact data.protection@admin.ox.ac.uk.

Under Principle 8, which restricts the transfer of material outside the European Area, personal data about an individual placed on the world wide web is likely to breach the provisions of the Act unless the individual whose data is used has given his or her express consent. It is important that all those preparing web pages, address lists and the like, are aware of these provisions, and seek advice from the Data Protection Officer if in doubt.

The Act specifies arrangements for the notification of processing undertaken by the Institution. The College has a wide ranging notification under the 1998 Act, which can be accessed online. Any members of staff who are uncertain as to whether their activities or proposed activities are included in the College's notification should contact the Data Protection Officer in the first instance.

A failure to comply with the provisions of the Act may render the College, or in certain circumstances the individuals involved, liable to prosecution as well as giving rise to civil liabilities. Individuals are encouraged to familiarise themselves with the general aspects of Data Protection contained in the College's guidelines to the Act, referred to above. Further information and advice may be obtained from College's Data Protection Officer.

Definitions

Data controller the person (or organisation) who determines the purposes for which and the manner in which any personal data are, or are to be, processed (e.g. the College).

Data subject any living individual who is the subject of personal data (e.g. student, applicant, member of staff, supervisor, referee etc).

Duty of confidentiality in the case of some subject access requests, the Data Protection Officer may have to take a decision on whether a document containing third party data was written in confidence and whether the breach of that confidence in releasing the document outweighs the requirement to comply with a subject access request.

Fair and lawful processing means one of the following conditions must be met:
The data subject has given his or her consent to the processing.

- The processing is necessary:
  (1) for the performance of a contract to which the data subject is a party; or
  (2) for the taking of steps at the request of the data subject with a view to entering into a contract.
- The processing is necessary to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
- The processing is necessary in order to protect the vital interests of the data subject.
- The processing is necessary for the administration of justice; for the exercise of any functions conferred by or under enactment; for the exercise of any functions of the Crown, a Minister of the Crown or a government department; for the exercise of any other functions of a public nature exercised in the public interest.
- The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject.

In the case of processing sensitive data, at least one of the following conditions must be satisfied (in addition to at least one of the conditions outlined above):

- The data subject has given explicit consent.
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred by law on the data controller in connection with employment.

Information Commissioner's Office the UK's independent authority set up to promote access to official information and to protect personal information.

Personal data data which relate to a living individual who can be identified from that information, or from that and other information which is in the possession of or is likely to come into the possession of, the data controller. It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (subject to very limited exceptions).

Processing obtaining, recording, holding or using the information or data (which includes, in relation to personal data, obtaining or recording the information to be contained in the data) or carrying out any operation or set of operation on the information or data. Under the new Act, processing is very

widely defined, to the extent that guidelines produced by the Information Commissioner suggest that it is difficult to envisage any action involving data which does not amount to processing within this definition.

Sensitive data information relating to race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life or criminal activities. Special conditions apply to the processing of this type of information, including an obligation to obtain the explicit consent of the individual (except in limited circumstances).

Third Party Information information relating to another individual (other than the data subject) who can be indentified by that information.

Principles

Organisations processing personal data must comply with the principles below:

First *Principle*

- **Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.**

Amongst the key conditions in Schedule 2 are that either the data controller has the consent of the data subject or the processing is necessary to fulfil a contract with the data subject or to comply with other legal obligations.

Special conditions apply to sensitive personal data, which is defined as information relating to race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life or criminal activities. These data cannot be processed in most circumstances unless the data subject has given explicit consent to the processing, or the processing is necessary for strictly limited purposes which are defined (e.g. the administration of justice).

Second Principle

- **Personal data shall be obtained for one or more lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**

It is important to be aware of the discipline that this implies. Material in a file may in the normal course of events be used for a number of purposes. It is now clear that use must adhere strictly to the purposes to which the attention of the data subject has been drawn.
Thus in future information obtained for the purpose of student records cannot be used for the purpose of, e.g., fund raising, unless the student has given prior consent.

Third Principle

- **Personal data shall be adequate, relevant and not excessive for the purpose or purposes for which they are processed.**

This implies not only that compiling too much information should be avoided, but also that sufficient information should be obtained for the proper performance of the operation.

Fourth Principle

- **Personal data shall be accurate and, where necessary, kept up to date.**

This principle requires that the data controller take reasonable steps to ensure the accuracy of data or, where the data subject has expressed a view that the data is inaccurate, that the data records that view.

Fifth Principle

- **Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.**

Sixth Principle

- **Personal data shall be processed in accordance with the rights of data subjects under this act.**

Seventh Principle

- **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

Thus data must be kept secure. It is the responsibility of the data controller to take reasonable steps to ensure the reliability of any employees who have access to personal data. In addition, if the data controller is using a third party processor then he must ensure that there is a contract in place with that data processor which provides for appropriate security measures.
Central administration, departments and faculties should consider the way in which manual as well as electronic data are held, to ensure that they comply with the requirements as to security.

Eighth Principle

- **Personal data shall not be transferred to a country or territory outside the European Economic Area (the 15 EU member states together with Norway, Iceland and Liechtenstein) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to processing of personal data. This principle does not apply where the data subject has given consent to the transfer or where the transfer is necessary for a contract with the data subject.**

Personal data published on the web is available to any country in the world, including those outside the European Economic Area. To avoid breaching the 8th principle, and to ensure that the processing is 'fair', as required by the 1stprinciple, personal data should not be placed on the web without the consent of the individual concerned.

Transfers of personal data to the United States were permitted under a 'Safe Harbor' agreement between the EU and the Unites States. However, in October 2015, the European Court of Justice ruled that the Safe Harbor agreement was no longer valid. For those wishing to transfer personal data to the

United States, the main alternatives are the adoption of contractual provisions that conform to 'model clauses' approved by the European Commission or transfers that are made with the consent of the individual.

Information for College staff on the processing of their personal data

In order to comply with its contractual, statutory, and management obligations and responsibilities, the College is required to process personal data relating to its employees, including 'sensitive' personal data, as defined in the Data Protection Act 1998 (the "Act") which includes information relating to health, racial or ethnic origin, and criminal convictions. All such data will be processed in accordance with the provisions of the Act and the College Policy on Data Protection as amended from time to time. For the purposes of the Act, the term 'processing' includes the initial collection of personal data, the holding and use of such data, as well as access and disclosure, through to final destruction. In certain circumstances, the provisions of the Act permit the College to process an employee's personal data, and, in certain circumstances, sensitive personal data, without their explicit consent. Further information on what data is collected and the purposes for which it is processed is given below.

Contractual responsibilities

The College's contractual responsibilities include those arising from the contract of employment. The data processed to meet contractual responsibilities includes, but is not limited to, data relating to: payroll; bank account; postal address; sick pay; leave; maternity pay; and pension and emergency contacts.

Statutory responsibilities

The College's statutory responsibilities are those imposed on the College by legislation. The data processed to meet statutory responsibilities includes, but is not limited to, data relating to: tax; national insurance; statutory sick pay; statutory maternity pay; family leave; work permits; and equal opportunities monitoring.

Management responsibilities

The College's management responsibilities are those necessary for the organisational functioning of the College. The data processed to meet management responsibilities includes, but is not limited to, data relating to: recruitment and employment; training and development; teaching; research; absence; disciplinary matters; health and safety; security, including College-operated CCTV; e-mail address and telephone number; swipe cards; and criminal convictions.

Sensitive personal data

The Act defines 'sensitive personal data' as information about racial or ethnic origin; political opinions; religious beliefs or other similar beliefs; trade union membership; physical or mental health; sexual life; and criminal allegations, proceedings or convictions. In certain limited circumstances, the Act permits the College to collect and process sensitive personal data without requiring the explicit

consent of the employee.

(a) The College will process data about an employee's health where it is necessary, for example, to record absence from work due to sickness, to pay statutory sick pay, and to make any necessary arrangements or adjustments to the workplace in the case of disability. This processing will not normally happen without the employee's knowledge and consent.

(b) Save in exceptional circumstances, the College will process data about an employee's racial and ethnic origin, their sexual orientation or their religious beliefs only where they have volunteered such data and only for the purpose of monitoring and upholding the College's equal opportunities policies and related provisions.

(c) Data about an employee's criminal convictions will be held as necessary.

Disclosure of personal data to other bodies

In order to perform its contractual and management responsibilities, the College may, from time to time, need to share an employee's personal data with one or more colleges. In such cases, the college or colleges will be required to process the data in accordance with the provisions of the Act.
For the performance of the employment contract, the College is required to transfer an employee's personal data to third parties, for example, to pension providers and HM Revenue & Customs.
In order to fulfil its statutory responsibilities, the College is required to provide some of an employee's personal data to government departments or agencies e.g. provision of salary and tax data to HM Revenue & Customs.

Some information about staff is sent in coded and anonymised form to the Higher Education Statistics Agency (HESA). Further information on how HESA uses this data is available from the HESA website.
The University will display an employee's webmail address and telephone number in the Online Contact Search Facility, which is accessible to internet users, including those in countries outside the European Economic Area (EEA). Employees should be aware that many countries outside the EEA do not have data protection legislation, or have different data protection or privacy regimes, and so may not always protect their personal data to the same standard as within the EEA. Requests to have an email address and/or telephone number omitted from the Online Contact Search Facility should be addressed to the employee's Telecommunications Co-ordinator (normally their departmental administrator) and will need to be approved by their Head of Department.

Keeping personal data up-to-date

The Act requires the College to take reasonable steps to ensure that any personal data it processes is accurate and up-to-date. It is the responsibility of the individual employee to inform the College of any changes to the personal data that they have supplied to it during the course of their employment.

Requesting information

Under the Act, it is possible for individuals to request access to any of their personal data held by the College, subject to certain restrictions. A request for disclosure of such information is called a subject

access request. Any such requests should be addressed to the Data Protection Officer.

Subject access requests

Under the Data Protection Act, individuals are entitled to seek access to their own personal data. Such requests are dealt with as subject access requests and are handled by the Data Protection Officer. It is important to ensure that any such requests are forwarded on to the Data Protection Officer ***promptly so that these can be dealt with within the 40-calendar-day deadline specified in the Act.***

Staff should be aware that in the event of a subject access request being made, the following documents are potentially disclosable:

- documents held in electronic/paper form;
- e-mails;
- handwritten notes;
- draft letters/documents, even where clearly marked as 'draft';
- references received by the College;
- examiners' comments; and
- other information identifying the individual making the request, for example by name, initials, photograph etc.

Just as draft documents are potentially disclosable, marking a document or e-mail as 'confidential' or 'strictly confidential' does not ensure that it will not be disclosable in the event of a subject access request.

It is therefore particularly important to ensure that only relevant and necessary personal information is collected, processed and retained. Careful consideration should be given as to when it is appropriate to write down information about individuals and whether e-mails, documents, draft letters etc need to be kept as part of the formal record or should be deleted.

Remember: any personal data the College holds is potentially disclosable, so before drafting an e-mail/minute/letter please bear in mind that the person to which it relates is entitled to ask to see it, and it may have to be disclosed to them.