Exeter College

Data protection policy

1. Introduction

Exeter College is fully committed to compliance with the requirements of the Data Protection Act 1998 (DPA), which came into force on 1 March 2000. The College subscribes fully to the University's policy on Data Protection, available at:

http://www.admin.ox.ac.uk/councilsec/dp/policy.shtml

We are required to maintain certain personal data about individuals for the purposes of satisfying our operational and legal obligations. We recognise the importance of correct and lawful treatment of personal data, as it helps to maintain confidence in our organisation and to ensure efficient and successful outcomes when using this data.

The types of personal data that we may process include information about current, past and prospective employees; clients and customers; suppliers and other organisations with whom we have dealings.

Personal data may consist of data kept on paper, computer or other electronic media, all of which is protected under the Data Protection Act 1998.

2. Principles

We endorse and adhere to the eight principles of the Data Protection Act, which are summarised as follows:

Data must:

1. be processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. be adequate, relevant and not excessive for those purposes.
4. be accurate and, where necessary, kept up-to-date.
5. only be kept for as long as is necessary for the purpose for which it was obtained.
6. be processed in accordance with the data subject's rights.
7. be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measure.
8. not be transferred to a country or 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.

These principles apply to obtaining, handling, processing, transportation and storage of personal data. Employees and agents of the College who obtain, handle, process, transport and store personal data for use must adhere to these principles at all times.

3. Types of data

The DPA lays down conditions for the processing of any personal data, and makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as data relating to a living individual who can be identified from that data; or from that data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an 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.

Sensitive personal data is defined as personal data consisting of information regarding an individual's racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; or criminal proceedings or convictions.

4. Handling of personal/sensitive information

The College will, through appropriate management and the use of strict criteria and controls:

- observe fully the conditions concerning the fair collection and use of personal information.
- specify the purpose for which information is used.
- collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements.
- endeavour always to ensure the quality of information used.
- not keep information for longer than required operationally or legally.
- always endeavour to safeguard personal information by physical and technical means (i.e. keeping paper files and other records or documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and computer systems by the use of secure passwords, which where possible, are changed periodically and ensuring that individual passwords are not easily compromised).
- ensure that personal information is not transferred abroad without suitable safeguards.
- ensure that the lawful rights of people about whom the information is held can be fully exercised.

In addition, the College will ensure that:

- there is someone with specific responsibility for data protection in the organisation (the designated Data Controller). The Data Controller is currently the Bursar of the College.
- all employees managing and handling personal information understand that they are contractually responsible for following good data protection practice.
- all employees managing and handling personal information are appropriately trained to do so.
- all employees managing and handling personal information are appropriately supervised.
- a clear procedure is in place for anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, and that such enquiries are promptly and courteously dealt with.
- methods of handling personal information are regularly assessed and evaluated.
- data sharing is carried out under a written agreement, setting out the scope and limits of the sharing.
- any disclosure of personal data will be in compliance with approved procedures.

Note that, by law, Exeter College has to provide employee liability information to any organisation that our employees are transferring to, in line with the Transfer of Undertakings Regulations.

5. Access to personal data

All individuals who are the subject of personal data held by us are entitled to:

- ask what information we hold about them and why.
- ask how to gain access to it.
- be informed how to keep it up-to-date.
- have inaccurate personal data corrected or removed.
- prevent us from processing information or request that it is stopped if the processing of such data is likely to cause substantial, unwarranted damage or distress to the individual or anyone else.
- require us to ensure that no decision which significantly affects an individual is solely based on an automated process for the purposes of evaluating matters relating to him/her, such as conduct or performance.
- be informed what we are doing to comply with our obligations under the Data Protection Act.

This right is subject to certain exemptions which are set out in the Data Protection Act. Any person who wishes to exercise this right should make the request in writing to the HR Officer. We reserve the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they will be amended upon request. If by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party.

Personal information will only be released to the individual to whom it relates. The disclosure of such information to anyone else without their consent may be a criminal offence. Any employee who is in doubt regarding a subject access request should check with the Data Controller. Information must under no circumstances be sent outside of the UK without the prior permission of the Data Controller.

We aim to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a written request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

6. Employee responsibilities

All employees must ensure that, in carrying out their duties, Exeter College is able to comply with its obligations under the DPA. In addition, each employee is responsible for:

- checking that any personal data that he/she provides to us is accurate and up to date.
- informing us of any changes to information previously provided, e.g. change of address.
- checking any information that we may send out from time to time, giving details of information that is being kept and processed.
- if, as part of their responsibilities, employees collect information about other people or about other employees they must comply with this policy. This includes ensuring the information is processed in accordance with the DPA, is only processed for the purposes for which it is held, is kept secure, and is not kept any longer than is necessary.

Employees are reminded that the DPA does not just apply to records held relating to our employees, but also to any client files/records. Information stored on clients should be reviewed regularly to ensure it is accurate and up to date. All documents, whether hand written or stored in emails (current or deleted) are potentially disclosable in the event of a request from an employee or client.

7. Data security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

All employees are responsible for ensuring that any personal data that they hold is kept securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

8. Publication of information

Information that is already in the public domain is exempt from the 1998 Act. This would include, for example, information on employees contained within externally circulated publications such as brochures and other sales and marketing aids.

Any individual who has good reason for wishing details in such publications to remain confidential should contact the Bursar.

9. Subject consent

The need to process data for normal purposes will be communicated to all data subjects.

Our contracts of employment require the consent of employees to the processing of personal data for the purposes of administering, managing and employing our staff. This includes: payroll, benefits, medical records, absence records, sick leave/pay information, performance reviews, disciplinary and grievance matters, pension provision, recruitment, family policies (maternity, paternity, adoption, etc.) and equal opportunities monitoring.

In some cases, if the data is sensitive, for example information about health, race or gender, express consent to process the data will be obtained. Such processing may be necessary to comply with some of our policies, such as health and safety and equal opportunities.

Information about an individual will only be kept for the purpose for which it was originally given. Employees and managers must not collect data that is simply "nice to have" or which is to be used for another purpose.

10. Retention and disposal of data

Information will be kept in line with our document retention guidelines. All employees are responsible for ensuring that information is not kept for longer than necessary.

Documents containing any personal information will be disposed of securely, and paper copies will be shredded.

11. Registration

Exeter College is registered in the Information Commissioner's public register of data controllers.

The Data Protection Act 1998 requires every data controller who is processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence. The Bursar is our Data Controller and is responsible for ensuring compliance with the Data Protection Act, for notifying and updating the Information Commissioner of our processing of personal data, and for the monitoring and implementation of this policy on behalf of Exeter College.

Any changes made to the information stored and processed must be brought to the attention of the Bursar immediately.

12. Implementation, monitoring and review of this policy

This policy will take effect from 1 September 2011. The Governing Body of the College has overall responsibility for implementing and monitoring this policy, which will be reviewed on a regular basis (at least annually) following its implementation and additionally whenever there are relevant changes in legislation or to our working practices.

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the HR Officer.

This policy is not contractual, but indicates how Exeter College intends to meet its legal responsibilities for data protection. Any breach will be taken seriously and may result in formal disciplinary action. Any employee who considers that the policy has been breached in any way should raise the matter with their Head of Department or the HR Officer.