

GREENHEAD COLLEGE

DATA PROTECTION POLICY

Data Controller (1): Mr Peter Gordziejko
Data Controller (2): Mrs Sue Creamer

Introduction

Greenhead College (the college) needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements and health & safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the college must comply with the Data Protection Principles which are set out in the Data Protection Act 1998.

In summary these state that that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- Be adequate, relevant and not excessive for those purposes
- Be accurate and kept up to date
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The college and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the college has developed the Data Protection Policy.

Status of the Policy

The policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the college from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

Responsibilities of Staff

All staff are responsible for

- Checking that any information that they provide to the college in connection with their employment is accurate and up to date.
- Informing the college of any changes to this information, e.g. change of address.
- Informing the college of any errors in their information.

Data Security

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Personal information should be

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or
- kept only on a disk which is itself kept securely.

Student Obligations

Students must ensure that all personal data provided to the college is accurate and up to date. They must ensure that changes of address, etc are notified to their tutor.

If they are using college computer facilities to process their personal data, they are responsible for its security.

Rights to Access Information

Staff, students and other users of the college have the right to access personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the college 'Access to Information' form, which is available on the college intranet, and give it to their line manager / personal tutor.

The college will make a charge of £10 on each occasion that access is requested, although the college has the discretion to waive this.

The college aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 days unless there is a good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

Publication of College Information

Information that is already in the public domain is exempt from the 1998 Act. It is the college's policy to make as much information public as possible, and in particular the following information will be available to the public.

- Names of college governors
- List of all staff
- Photographs of staff
- Student examination results
- Student destinations
- Photographs of students

It is the college's policy to make as much information public as possible. Access to public information is to be available under the Freedom of Information Act 2000.

The college internal phone list will not be a public document

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the designated data controller.

Subject Consent

In many cases the college can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express written consent must be obtained. Agreement to the college processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

College staff will be in contact with young people between the ages of 16-19. The college has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the course offered. The college has a duty of care to all staff and students and must therefore make sure that employees and those who use the college facilities do not pose a threat or danger to other users.

The college will also ask for information about particular health needs, such as allergies, or conditions such as asthma or diabetes. The college will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

Therefore, all prospective staff will be asked to sign a consent to process form and students will be asked to sign a declaration on their learning agreement.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the college is a safe place for everyone, or to operate other college policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and

students will be asked to give express consent for the college to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to, this without good reason.

The Data Controller

The college as a corporate body is the data controller under the Act, and the board is therefore ultimately responsible for implementation. However, the designated data controllers will deal with day-to-day matters.

The college has two designated data controllers. They are named on the top of this document.

Retention of Data

The college will keep some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. In general, information about students will be kept for a maximum of 10 years after they leave college. This will include

- name and address
- academic achievements
- copies of any reference written
- copies of job/course application forms
- progress reports.

All other information, including any information about health, race or disciplinary matters will be destroyed within 6 months of the course ending, except in instances where this data is retained by the Equal Opportunities Co-ordinator for statistical purposes.

The college will also need to keep information about staff for longer periods of time. In general, all information will be kept for 10 years after a member of staff leaves the college. Some information will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. A full list is available from the data controller.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the college. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to college facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy would be taken up with the designated data controller.

Approved by the Governing body – 29 June 2009