REASEHEATH COLLEGE

Data Protection Policy

The College needs to keep information about its students, employees and other users to allow it to monitor performance, achievements, health and safety and to comply with obligations to funding bodies and the government. To comply with the law, information must be collected and used fairly, safely stored and not disclosed to any other person unlawfully. This Policy addresses the College's response to comply with the Data Protection Act, 1998.

Introduction

The College must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state 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 this Data Protection Policy.

Status of the Policy

This 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 failure to follow the policy can therefore result in disciplinary proceedings. In addition to this general policy there is a Staff Data Protection Policy which is available on the intranet and is reproduced as Appendix 4 to this document.

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 their Line Manager, Section Leader or the HR Manager. If the matter is not resolved it can be raised as a formal grievance.

Notification of Data Held and Processed

All staff, students and other users are entitled to:

Know what information the College holds and processes about them and why.

Know how to gain access to it.

Know how to keep it up-to-date.

- Know what the College is doing to comply with its obligations under the 1998 Act.

On request, the College will provide staff and students and other relevant users with a standard form of notification. This will state all the types of data the College holds and processes about them, and the reasons for which it is processed.

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 information, which they have provided ie change of address.
- Checking the information that the College will send out from time to time, giving details of information kept and processed about staff.

Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

If and when, as part of their responsibilities, staff collect information about other people, (ie about students course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff, which are at Appendix 1.

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.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a locked filing cabinet, drawer, cupboard or room;
- Not be visible to anyone not authorised to see it, either on desks or on computer screens;
- if it is computerised, be password protected (including the use of password protected screen savers);
- if transmitted through the internal mail, be sent in a sealed envelope, and labelled as Private and Confidential;
- if transmitted through the post externally, be sent in a sealed envelope, labelled as Private and Confidential Addressee Only and by posted as special delivery;
- Not be sent by e-mail if it sensitive personal data;

Personal data should not be put on laptops, CD-ROM/DVD devices, memory sticks or other portable media unless they are registered encrypted devices.

Staff wishing to use documents or files stored on network drives while off-site should use the Whale Access Gateway Device or the VMWare Virtual Desktop system to access such documents or files.

More information on encrypted devices, the Whale Access Gateway and the VMWare Virtual Desktop system is available from IT Services.

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 the student registry as appropriate.

Students who use the College facilities may undertake tasks which involve the processing of personal data. If they do they must notify the data controller. Any student who requires further clarification about this should contact the data controller.

Rights to Access Information

Staff, students and other users of the College have the right to access any 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 and send it to the Associate Director.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing using the standard form attached (see Appendix 2).

The College will make a charge of £10 on each occasion that access is requested, although the College has discretion to waive this. Charges will not be made for information requests made outside the scope of the policy (such as routine staff requests for information from the Personnel Officer).

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 good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

Publication of College Information

Information that is already in the public domain is exempt from the 1998 Act. It is the policy of the College to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Names and contact of the College's governors
- List of staff
- Agendas and minutes of Governing Body meetings

Any individual who has good reason for wanting details in these lists or categories to remain confidential should contact the HR Manager.

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 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.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages to 16 and 18. 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 courses offered. The College also 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 to particular forms of medication, or any 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.

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 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 and the Designated Data Controllers

The College as a body corporate is the data controller under the Act, and the board is therefore ultimately responsible for implementation. The designated data controller is the Head of Technical Services.

Examination Marks

Students will be entitled to information about their marks for both course work and examinations. However, this may take longer than other information to provide. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned to the College.

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. In general personal information about students will be kept for six years after they leave the College but course lists of names of students and final examination results will be kept in perpetuity. This will include

- name and address

- academic achievements, including marks for course work and
- copies of any reference written

All other information, including any information about health, race or disciplinary matters will as far as is possible be destroyed within 6 years of the course ending and the student leaving the College.

Staff information will be retained as set out in the Staff Data Protection Policy.

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 the College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated data controller.

Note

The following documents are appendices to this policy:

Staff Guidelines for Data Protection.
Request Form for Data Access.
Advice on the Disclosure of Personal Data.
Staff Data Protection Policy.

Author/Reviewer	Head of Technical Services
Date of last revision	February 2013
Authorising body/Date	College Board / March 2003
Date of next review	February 2016
Initial Impact Assessment	February 2010
Published on: Staff Intranet, Student Intranet, College website	

DATA PROTECTION POLICY Appendix 1

Staff Guidelines for Data Protection

All staff will process data about students on a regular basis, when marking registers, writing reports or references, or as part of a pastoral or academic supervisory role etc. The College will ensure through registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 1998 Act. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

General personal details such as name and address.

- Details about class attendance, course work marks and grades and associated comments.
- Notes of personal supervision, including matters about behaviour and discipline.

Information about a student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the students consent eg recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties.

All staff have a duty to make sure that they comply with the data protection principles, which are set out in the Data Protection Policy. In particular, staff must ensure that records are:

- accurate
- up-to-date
- fair
- kept and disposed of safely, and in accordance with the College policy.

The College will designate staff in each area as 'authorised staff'. These staff are the only staff authorised to hold or process data that is:

not standard data; or
sensitive data

The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary:

- in the best interest of the student or staff member, or a third person, or the College

- he or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.

  This should only happen in very limited circumstances eg a student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student is pregnant or a Jehovah's Witness.

Authorised staff will be responsible for ensuring that all data is kept securely.

Staff must not disclose personal data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with the College policy.

Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with the College policy.

Before processing any personal data, all staff should consider the checklist.

Staff Checklist for Recording Data

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interest of the student or the staff member to collect and retain the data?
- Have you reported the fact of data collection to the authorised person within the required time?

DATA PROTECTION POLICY **Appendix 2**

Standard Request Form for Access to Data

I …….. wish to have access to either:

*Delete as appropriate

*1. All the data that Reaseheath College currently has about me, either as part of an automated system or part of a relevant filing system; or

*2. Data that Reaseheath College has about me in the following categories:

Academic marks or course work details

Academic or employment references

- Disciplinary records
- Health and medical matters
- Political, religious or trade union information
- Any statements of opinion about my abilities or performance
- Personal details including name, address, date of birth etc
- Other information

(Please tick as appropriate)

I understand that I will have to pay a fee of £10 in advance.

Signed: …….. Date of Birth: …….

Date: …….. Telephone No: …….

Address to which information is to be sent:

…….

…….

…….

…….

Appendix 3

DATA PROTECTION ACT 1998

ADVICE ON THE DISCLOSURE OF PERSONAL DATA

1. Introduction

1.1 The following advice is intended to help establish procedures within the College that will enable staff to deal more easily and consistently with requests for a disclosure of personal data. These requests for information will come from "Data Subjects", who are the individuals to whom the personal data relate; from within the organisation; or from Third Parties who can be anybody else.

1.2 In the first and last cases, the procedures outlined in Section 2 below must be adhered to before personal data can be disclosed. However, internal disclosures of personal data can take place for bona fide purposes connected with the College's (ie the Data User's) functions.

1.3 In general, a disclosure must only take place if one of the following conditions applies:

when the permission of the Data Subject has been given

within the College, for the authorised functions or registered purposes of the College

to persons registered under the Data Protection Act as recipients (disclosure) of the College's personal data

where the disclosure is by order of a Court, or a statutory duty

2. Disclosing Personal Data on the Telephone

2.1 When requests for personal data are received on the telephone, staff should not disclose any personal data without first seeking the approval of a College Director.

2.2 Even where approval is given, staff should not disclose information over the telephone before the caller's identity has been verified (eg by phoning them back on a known number, or by confirming a known reference number, or by discussing some reference details known only to the Data User and the caller). This may be difficult if the caller is agitated or angry, but usually callers will divulge information that will help to assess their true identity.

2.3 If the caller is insistent or 'difficult', staff should ask whether it is possible for the caller to phone again, or to be phoned back at a later stage, or whether the caller can wait until staff can consult their line manager.

2.4 If common sense suggests that a particular disclosure should be an exception to the rule (eg where someone might be at risk), staff should make a proper record of the disclosure, to whom it was made, and of the circumstances that made the disclosure necessary. See Section 7 for further details.

2.5 Where disclosures of sensitive information take place a note of the disclosure should be recorded on the appropriate files or case papers.

2.6 Staff should ensure that all requests for personal data outside their normal duties, are approved before the request is satisfied.

2.7 Staff should note that the confidential nature of any personal information supplied must be stressed at all times; so they should not take short cuts and always following the correct procedure. **If in doubt, do not disclose.**

3. Refusing to Disclose Personal Data

3.1 Where disclosures of data is refused, staff should explain they are not allowed to disclose personal data unless the caller's credentials to receive the data have first been verified. Staff should always explain that the reason why they are refusing to give information is one of confidentiality, and because the caller has not provided adequate identification. The following is suggested as the basis for a standard explanation:

"The 1998 Data Protection Act regulated the use of personal data. It is the College's policy to respect the confidentiality of the personal data in its possession, and because you have not been able to identify yourself properly, I cannot help you. However, if you can call again, and provide satisfactory identification, I will be able to comply with your request."

4. Forwarding Letters

4.1 In some circumstances, staff may wish to offer to forward letters on behalf of the enquirer, but they should make it clear that they can give no guarantee of locating the person in question.

4.2 Staff should ask the enquirer to enclose the letter in a sealed envelope, and to provide a stamped envelope endorsed with the name of the recipient, together with a formal written request for the letter to be forwarded. This request should contain the last known whereabouts of the recipient, and should be marked for the attention of the Programme Area who will deal with the request.

4.3 Staff should ensure that the letter to be forwarded is accompanied by a compliment slip explaining this action, and stressing that the recipient's address has not been disclosed to the writer of the letter.

5. Disclosures of Personal Data to Prosecuting Agencies

5.1 If staff receive a request for personal data from a police officer, customs official etc, they should refer the request to an appropriate Director or Residential Services Manager. As disclosures to prosecuting agencies can be controversial, the reasoning behind the procedure is fully explained below. Note that where the College has a statutory duty to provide such personal data to these agencies, or if the data are not personal data under the Data Protection Act, or if disclosures to these agencies have been registered under the Act, then the following procedures need to be followed.

5.2 Section 28 of the Data Protection Act allows for personal data to be disclosed to certain agencies (eg Police, Inland Revenue, Customs and Excise, Public Health Authority, etc) for the purposes of:

(a) the prevention of detection of crime;

(b) the apprehension of prosecution of offenders; or

(c) the assessment or collection of any tax or duty

without fear of making an unauthorised disclosure so long as Data Users can prove that they 'had reasonable grounds for believing that failure to make the disclosure in question would have been likely to prejudice any of those matters'. (See (a), (b) and (c) above).

5.3 It is likely that only agencies with a statutory duty to investigate the matters mentioned in (a), (b) and (c) above will use this Section of the Data Protection Act. Note that there is no compulsion to comply with a request for personal data under this Section, and a request can be refused.

5.4 In practice, the Police (for example) are expecting to be required by Data Users to state in writing that their officers have requested the personal data for the purpose (a), (b) or (c) above. Thus it is suggested that, to be consistent, all agencies who may want the Data User to disclose personal data under Section 28 of the Data Protection Act should be required to present a request in writing. Disclosures of personal data to prosecuting agencies should not be made orally.

5.5 The procedure for disclosure would be:

(a) the request for disclosure must be received in writing from the agency, and must explain why personal data are required by the agency

(b) the disclosure is discussed by senior management

5.6 If the disclosure is approved, management should make a formal record of the decision and file this with the written request required. The record should include the time and date of the approval, who made the decision, who was involved in the discussions about the disclosure, and a copy of the personal data disclosed.

5.7 If the disclosure is denied, a formal note explaining why the personal data were not released should be sent to the agency.

5.8 If anyone is unsure what to do he/she should:

discuss the matter with an appropriate Director.

attempt to find out more information from the agency as to why the personal data are required.

6. Calling in a Prosecuting Agency

6.1 The procedures mentioned in Section 5 above still apply if a senior manager discovers a crime and calls the Police in. For example, an auditor as part of his routine work may come across an irregularity that warrants Police involvement. At this juncture the auditor will want the evidence to be put in the hands of the Police to enable them to apprehend the culprit, and this could involve the disclosure of personal data.

6.2 As before, when such a disclosure does take place, it will be necessary to take note of details of the meeting, who was present, the nature of the irregularity and what personal data were disclosed to the Police.

7. Emergencies

7.1 There may be circumstances where staff have to disclose personal data in emergencies. If an emergency involves a threat to a Data Subject's health or to prevent injury to a Data Subject, then the disclosure can take place.

7.2 A proper record of the disclosure must be made, either at the time, or as soon as possible after the disclosure has occurred. In other urgent situations, staff will have to use their judgement; but in all cases they should keep a formal record of their decision to disclose.

8. 'Subject Access' to Personal Data

8.1 Staff may be consulted by an individual who wishes to apply formally for Subject Access. In these cases, the Data Subject should be referred to the HR Manager.

8.2 All staff should be aware that Subject Access is a separate and formal procedure by which personal data are disclosed to the Data Subject.

9. Access to Personal Data by Governors

9.1 Staff should refer any request for personal data, from Governors, to their line manager, as disclosures of this kind can be difficult to handle.

A Governor, by virtue of office, is entitled to have access to all documents in possession of the college as far as such access if reasonably necessary to enable her/him properly to perform her/his duties

A Governor has no 'roving commission' in respect of local College documents and mere curiosity is not a sufficient basis for access to information

In the case of a Committee of which the Governor is a member, there is a presumption that the Governor has good reason for access to all the information and documents which pertain to the functions of that particular Committee

In the case of a Committee of which the Governor is not a member, he has no automatic right of access to material and has to demonstrate a 'need to know'

The decision about whether a Governor has good reason for access to the material of a Committee of which he is not a member is ultimately one to be taken by the Governing Body themselves, but the Governing Body can delegate to the Clerk to the Governors the right to decide whether an application for access to material ought to be granted, subject, however, to the Governors having a right of appeal to the Chairman.

10. Common Law Duty of Confidentiality

The Data Protection Act is not the only restriction on disclosure of information on the College. It is also bound by a common law duty of confidentiality. This duty prevents the College from releasing information about staff and students without their consent. This duty applies to manual records as well as information held on computers, and is therefore, broader than the DPA. Information which must be treated as confidential includes the names and addresses of employees and students and any other information about them which is not publicly known. Accordingly, to ensure that we do not breach our duty, no information, even if it only exists in printed form, should be disclosed unless all the relevant procedures have been followed.