DATA PROTECTION POLICY

Purpose of Policy/ Document

To ensure that HoW college satisfies the requirements of the Data Protection Act **To safeguard the personal information of students, staff and other clients** **To alert staff and students to the importance of protecting personal data, and informing them of the actions they need to take**

Application of Policy (Range and Scope)

The policy applies to all staff, students, potential students who enquire or apply, applicants to staff posts, any others who act on behalf of the college. We are also responsible for the actions of all subcontractors in relation to the personal data held on college clients.

Links

Safeguarding Policy
Recruitment and Selection of Staff Policy
Sickness Absence Policy
Maternity Policy
Document Retention Policy

Particular Legal Requirements/Issues Outside of Equality, Diversity and Disability (E.D.D)

Requirement to satisfy the Data Protection Act
Equality, Diversity and Disability (Disability, Equality, Duty Impact Assessment)

Has a Preliminary Equality Analysis been completed?

Yes **Date Completed: 12.03.16**

Is a full Impact Assessment required?

No

If 'yes', has a copy been sent to the Student Experience Manager?

N/A

For Completion by the Executive:

POLICY REFERENCE	**MIS01**
CATEGORY	**MIS**
AUTHOR / ORIGINATOR	**John Littler**
ISSUE DATE	**October 2015**
REVIEW DATE	**October 2017**
POSTHOLDER RESPONSIBLE FOR REVIEW	**John Littler**
RATIFIED /AUTHORISED BY	**Corporation**

HEART OF
WORCESTERSHIRE
COLLEGE

Data Protection Policy

Background.

The information on the 1998 Data Protection Act, and the legal interpretation is based on the guidance provided by JISC Legal in the booklet entitled "Code of Practice for the Further and Higher Education Sectors on the Data Protection Act 1998, which can be accessed at: http://www.jisclegal.ac.uk/Portals/12/Documents/PDFs/DPACodeofpractice.pdf and the JISC document "Data Protection and Research Data" which can be accessed at https://www.jisc.ac.uk/guides/data-protection-and-research-data

The JISC Legal document provides very detailed guidance on all aspects of the act that are relevant to Further Education Colleges. Answers to individual questions can also be obtained from the Information Commissioner's Office (ICO)

Contents

1. POLICY AND PROCEDURES

1.1. The Data Protection Act 1998 came into force on 1 March 2000. It is concerned with the rights of individuals to gain access to personal information held about them by an organisation or individual within it, and the right to challenge the accuracy of data held. The terms of the Act relate to data held in **any** form, including written notes and records, not just electronic data.

This document summarises the implication of the Data Protection Act for the College, sets out the College's general Policy on adherence to the Act, and offers specific guidance relating to:

- Procurement, storage, disposal and release of personal data;
- Examination procedures;
- Supplying, requesting and receiving 'confidential' references;
- Applications and interviews;
- Research involving data from human participants;

- Medical data.

It is not possible to cover all activities that individuals or departments might engage in. Guidance relating to some other matters can be found in the sources mentioned in the next paragraph. If in doubt contact the College's Data Protection Officer.

1.2. ***The 8 data protection principles***. The Act requires that all staff and others who process or use any personal information must ensure that they adhere to the **8 data protection principles**. In summary these require that personal data, including sensitive 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
- 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.

1.3. ***Definition of 'data'***. In the terms of the Act, **data** are information relating to an individual where the structure of the data allows information about the individual to be readily accessed. The information may be held in manual form (e.g., as written notes relating to a person or as part of a filing system, including card index or filing cabinets structured by name, address or other identifier) or in a form capable of being processed electronically. **Personal data** are any data relating to a living individual (e.g., name, address, payroll details, exam results). Anonymous data which cannot be tracked linked to a living person is not defined as personal data, however care should be taken to ensure small data sets cannot identified. **Sensitive data** form a subset of personal data that relate to a living person, recording such attributes as racial or ethnic origin, sexual life, political opinions, religious beliefs, trade union membership, health, criminal convictions, etc. Data are processed whenever compiled, stored or otherwise operated upon. Similarly, data about staff are processed when they are committed to manual or electronic records held within the institution.

1.4. ***Notification***. Under the Act the College as a data controller is required to notify the Information Commissioner of certain details of the processing of personal data by the College. The College's details are used by the Commissioner to make an entry describing the processing in a register which is available to the public for inspection. You can find the college's registration on the Information Commissioner's (ICO) website.

1.5. ***Making a 'data subject enquiry'***. Subject to a limited number of statutory restrictions, an individual or **data subject** (who could, for example, be a past or present student or member of staff of any category) can request to see whatever personal / sensitive information are held on them within the College. They can do this by filling out a Data Subject Enquiry form available on application to the Data Protection Officer, and submitting it, together with a small fee (currently £10) and proof of identity, to the Data Protection Officer who will then co-ordinate access to such

data as is held within the whole of the institution. This is to ensure that it is treated correctly to meet the legal requirements, and also because data relating to an individual may be held in several different places within the College.

2. GENERAL GUIDELINES

2.1. ***Procuring personal data***. The Act does not allow an individual to prevent an organisation from making reasonable use of personal data in the interests of providing an education or employment. For example, staff and students must expect certain information about them to be placed in the public domain (telephone extension number, college affiliation, email address, digital image, etc). Any permission to process staff/student information necessary in accordance with the College's contract to provide education or employment will be obtained by the MIS Department at the start of the contract (e.g. receipt of Application Form or Enrolment Form). Principle 3 of the Act requires, however, that only necessary data shall be collected. Departments should ensure that they only collect data on individuals that are necessary for the effective functioning of the institution or section. Procedures should be reviewed at intervals to ensure that this is the case, and that unnecessary information is not being requested or retained.

2.2. ***Storing personal data***. Personal data must be held securely. In the case of manual data this could be in filing cabinets, locked cupboards or rooms with access restricted to named individuals or categories of individual only. In the case of electronic information, access should be subject to reasonable controls, which might include passwords, encryption, compartmentalised access and access logs. Reasonable steps should be taken to detect and prevent unauthorised access. Personal data must not be stored on portable devices such as laptops, memory sticks, smart phones or tablets. However VPN access to college servers is provided when staff work off site further advice can be obtained from the I.T. Services Support team. The recommended retention periods can be obtained from the college retention policy.

2.3. ***Disclosing personal data***. Personal data should not generally be disclosed to third parties without the permission of the individual concerned. In this context, "third parties" includes family members, friends, local authorities, government bodies and the police, unless disclosure is exempted by the 1998 Act or by other legislation. Under certain circumstances, data may however be released. Note that among other circumstances the Act permits release of data without express consent:

- for the purpose of protecting the vital interests of the individual (e.g., release of medical data where failure to do so could result in harm to, or the death of, the individual);
- for the prevention or detection of crime;
- for the apprehension or prosecution of offenders;
- for the discharge of regulatory functions, including securing the health, safety and welfare of persons at work;
- where the disclosure is required by legislation, by any rule of law, or by the order of a court.

Most bodies that may request personal data in such circumstances should be able to provide documentary evidence to support their request. The absence of such documentation or a warrant may justify refusal to disclose personal data. Any such disclosures should only be made with the agreement of the College Data Protection Officer.

2.3.1. ***Employment agencies and prospective employers***. A further issue arises where employment agencies or prospective employers contact institutions to verify details about an individual, such as

attendance records, examination results, and degree classifications. In most circumstances, the individual concerned would not object to the disclosure of such information, and indeed it would appear to benefit the individual. However, care should at least be taken to ensure that the third party has a genuine requirement for the information. Depending on the sensitivity of the data being sought it may be appropriate to seek evidence of consent having been given by the person to whom the data relate.

2.3.2. ***Disclosure to third parties***. As a rule, personal or sensitive data should not be disclosed without the express consent of the individual concerned. If staff receive a phone call from a third party requesting information on a member of staff or student they should not disclose any information about the individual, however hard the caller may press. They should explain that the College does not discuss individuals without the express permission of the individual concerned. They should assure the caller of their willingness to help. Offer to attempt to contact the person concerned and take details of the request for information, including the caller's number. Offer to phone the caller back if necessary (this also offers some measure of authentication of the caller). If necessary, ask them to put their request in writing. Offer to accept a sealed envelope for the Department to forward to the individual concerned. Follow similar guidelines when dealing with written requests for information.

2.3.4. ***Emergencies and dealings with the police***. All police requests should be referred to the HR Manager if it involves a member of staff, or to the Assistant Principal of Support, Skills & Progression or the Student Services Manager if it involves a student. In every case the Data Protection Officer must be informed. Normally the college would respond positively, but the college has the right to withhold the information.

JISC guidelines indicate that it is not necessary to obtain explicit permission from next of kin etc. to store their contact details for use in the event of emergencies, though that information should be kept secure and destroyed when it is no longer needed.

2.4. ***Protecting third parties***. In meeting a data subject access request, it is important that personal data relating to other identifiable individuals mentioned in the documents (e.g., other staff or students) should not also be revealed unless permission for disclosure is given by the individual(s) concerned. Thus, a data subject enquirer has the right to see notes or comments relating to them that are held by the College in manual or electronic form, but the identity of the individual(s) who made those comments should not be revealed without their express permission.

2.5. ***Disposal of personal data***. Personal data should be disposed of when no longer needed for the effective functioning of the institution and its members. The method of disposal should be appropriate to the sensitivity of the data. Information regarding secure disposal of paper records or Electronic Data should be obtained from the college Document Retention Policy

Further information on college protocols on confidentiality and information –sharing can be found in the Confidentiality Policy and Safeguarding Policy.

3. EXAMINATIONS

3.1. ***Exam scripts and comments on scripts***. Examination scripts are exempt from data subject access because they are statements from the students, not data about them. Hence a student could not use the Act to obtain a copy of an exam script they had produced. However examiner's comments on the content of scripts **are** disclosable, whether recorded on the script or held separately. All comments

committed to writing should therefore be fair and defensible and should relate to the script rather than the student. For external examinations, the College Examination Policy, JCQ Procedures and Awarding Body procedures must be followed.

3.2. ***Publishing examination results***. The practice of publishing examination results via posting on notice boards or inclusion in the local press is only permissible if consent is obtained from the candidates. Students have the right to withhold such consent. If a student wishes to obtain results by telephone, then results can only be disclosed if the identity of the person requesting the details can be satisfactorily established.

4. CONFIDENTIAL REFERENCES AND INTERVIEWS

The precise application of the Act to the giving, requesting and receiving of 'confidential' references is not entirely clear, and is the subject of ongoing discussion. If in doubt, please seek advice from the College's Data Protection Officer, the HR Manager or Assistant Principal Support, Skills and Progression as appropriate.

4.1. ***Supplying personal references***. Personal references (and other personal data) supplied for specified purposes, including education, training or employment, are exempt from subject access. Thus, if you write a 'confidential' reference for an individual, you cannot be required to disclose its contents in response to a data subject enquiry.

The exemption from disclosure does not, however, apply to the individual or organisation that receives the reference. They can be expected to disclose a reference, particularly if they judge that it is possible to conceal the identity of the referee (e.g., by blanking out their name, address, etc). If it is not possible for the identity of the referee to be concealed, then they should not disclose the reference without the express consent of the supplier, because to do so would be to disclose personal data about the supplier.

Notes made in the course of interviews constitute individual data and are therefore subject to access under the Act. They should be fair, reasonable and defensible.

Please consult the document "Recruitment and Selection of Staff Policy" on the staff portal at https://portal.howcollege.ac.uk/policies/Policies/Forms/AllItems.aspx for more information

5. PHOTOGRAPHS, VIDEO AND CLOSED-CIRCUIT TELEVISION

Images of identifiable individuals constitute personal data in terms of the Act. Photographs of individuals should not be displayed in departments, used in teaching material, promotional material, prospectuses, etc., displayed on web sites, or in any other way made public without the permission of the individual(s) concerned. The same restrictions apply to video images (or audio recordings) used, for example, in teaching or promotion. If you are allowing others to take photographs or videos at any event you are organising, you are advised to mention this in your publicity and advise those who are attending in advance. If they object for any reason, it is up to you to ensure that they are not photographed or videoed.

The College employs closed-circuit television as part of its security systems. This will be done within the Code of Practice on the use of CCTV issued by the Office of the Information Commissioner.

6. **MARKETING INFORMATION**

Personal data relating to students or other members of the College past or present should not be passed to marketing organisations without the student's express permission.

7. **RESEARCH**

It is important that all members of the College involved in collecting data from human participants appreciate the importance of ensuring that their procedures comply with the requirements of the Act.

8. **MEDICAL AND SICKNESS RECORDS**

Information under this heading is 'sensitive data'. Doctors or persons with an equivalent duty of confidentiality (student counsellors etc.) can hold data without contravening the law. Oral discussion is not subject to data protection regulations where no written record exists. Central administration will seek consent from staff and students to pass on vital medical information in cases of accident or special circumstances.

9 RESPONSIBILITIES

Students

Students must ensure that any information they provide to the College is accurate and is kept up-to-date.

If they find themselves in a position where they are processing personal data about staff or other students (e.g., as a student representative on a College committee or group, or as the secretary of a society), they must ensure that they comply with College Policy and with the requirements of the Act.

If a student participates in research involving personal data, they must understand and fully comply with the law.

Staff

Staff must ensure that any information they provide to the College in connection with their employment is accurate and up-to-date and respond to any checks the college may carry out periodically.

Staff must be aware of the basic principles of the act as outlined in section 1.2 and understand that failure to comply could result in either a corporate prosecution or a personal prosecution, and failure to follow the guidelines could result in disciplinary proceedings.

Staff must respect the privacy and confidentiality rights of all data subjects. They must ensure that personal information is not disclosed to any unauthorised third party. They must ensure that third parties do not access personal data through casual access (e.g. via computer screens or leaving personal data lying in a public place).

Staff must ensure all data to which they have access is secure, (e.g. paper records in a classroom are locked in a filing cabinet) and that IT security policies are followed, including protection of passwords.

Staff must observe the college policy detailed in paragraph 2.2 which prohibits the storage of personal data on portable storage devices.

Staff should not collect or store personal data from students without the agreement of the data protection manager, who will also ensure that the required data protection statements are provided on collection documents. Wherever possible, personal data should be collected and stored in central systems such as UNIT-e, Spirals, ProMonitor or the HR system.

Data Protection Officer

The Officer will

Maintain the ICO notification view and update the policy every 2 years, and provide the Corporation with an annual report on compliance

Monitor all subject access requests to ensure compliance, advise on non-routine requests for personal information, and ensure that adequate guidance is available to staff.

Senior Leadership Team

The Senior Leadership Team should review Data Protection Policy every two years, and will review an annual report summarising data requests, training programmes, compliance and adherence to the ICO notification.