Huddersfield New College Further Education Corporation

Data Protection Policy

Section 1 – Introduction

Purpose and Scope

This Data Protection Policy ("the **Policy**") gives detailed guidance and instruction on how the Huddersfield New College ("the College") will process personal information about its staff, students, students' parents, suppliers and, where appropriate, other workers. The Policy also sets out how staff, and where appropriate, students, students' parents, suppliers and other workers must ensure that all Personal Data (as defined below) is processed correctly and lawfully.

Whilst it is important to note that this Policy applies to all staff, students, students' parents, suppliers, volunteers and other workers, there will be certain sections of this Policy which will be targeted solely at those who handle Personal Data at the College. Unless otherwise applicable, all references to staff includes all current, past and prospective staff, full time and part time staff as well as supply staff, contractors and volunteers. Unless otherwise applicable, all references to students includes all current, past and prospective students, whether full-time or part-time.

This Policy is designed to provide user-friendly and accessible information and guidance to ensure that staff and students understand the College's procedures and the law surrounding data protection. The law requires the College to protect the information that it acquires, uses and holds about identified or identifiable individuals.

The College will at all times seek to ensure that the practices that it employs comply with the required standards under both law and any applicable guidance issued by the Information Commissioner's Office ("**ICO**"), which is the governing body for data protection matters.

If you have any questions about this Policy, or if you have any issues which are not resolved by this Policy then you should contact the Data Protection Officer Julie Pryce on info@huddnewcoll.ac.uk.

This Policy does not form part of the terms and conditions of employment for any employee of the College. However, staff are expected to abide by this policy and may be subject to disciplinary procedures if found to be in breach of it.

General Policy Statement

In order to operate efficiently and to fulfil many of its functional as well as legal obligations, the College needs to collect and use certain types of information about the people with whom it deals. These include current, past and prospective staff, students, suppliers, and others with whom it communicates. This personal information must be dealt with properly however it is collected, recorded and used – whether in physical paper files, stored on a computer, or recorded in some other method. All information containing Personal Data must be carefully classified to ascertain what type of Personal Data it is and protected against unauthorised access, accidental loss or destruction, modification or disclosure to any third parties.

The College regards the lawful and correct treatment of Personal Data as important to successful operations, and to maintaining confidence between those with whom we deal and ourselves. To this end we are committed to the eight principles of data protection, as stated in the Data Protection Act 1998 ("**the Act**").

Definitions

All of these terms are defined under the Act:

Personal Data

"Personal Data" means data relating to a living individual who can be identified:

- from those data; or
- from those data 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 that individual.

Sensitive Personal Data

"Sensitive personal data" consists of personal data relating to ethnic origin, physical and mental health (including, for example, how many days sick leave an individual has had), sexual orientation, religion or belief, political opinion and information relating to alleged or actual criminal offences. The more sensitive the data is, the more securely it should be treated in terms of deciding whether it is necessary to obtain it, how to obtain it, whether to retain/disclose it, how long to retain it for and how to retain/disclose it. The sensitivity of the data will often depend on the person receiving the data and the circumstances under which they are receiving it.

Processing

"Processing" means obtaining, recording, holding or adding to the information or data or carrying out any operation or set of operations on the information or data. All Personal Data shall be retained in accordance with the provisions in Appendix C.

Data Subject

"Data Subject" means an individual who is the subject of the personal data.

Data Controller

"Data Controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. In this case, the College or individuals acting on behalf and with the authority of the College (See *Appendix J)*

Data Processor

"Data Processor" means any person who processes the data on behalf of the College. This includes a member of staff, or any third parties who are sub-contracted to carry out any services for or on behalf of the College and have access to personal data.

Information Commissioner

The Information Commissioner oversees the implementation of the Act (See *AppendixJ*).

Section 2 – Data Protection Principles

This Policy aims to ensure that the College complies with the eight data protection principles set out in Schedule 1 of the Act which state that Personal Data::

i. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met. For example, staff making decisions on enrolment using student application forms should do so without discriminating against any student.

ii. Shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. For example, student applications should be obtained for making application decisions and retained in the event of any appeals against those decisions.

iii. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. For example, it would be adequate and relevant to request details of a student's grades from their previous school to make a decision about whether or not to allow them to take a certain course, but might not be adequate or relevant to request information about their father's occupation.

iv. Shall be accurate and, where necessary, kept up to date. For example, it is extremely important that the College is kept up to date on any medical issues the student may have (such as allergies or medication that they are required to take).

v. Shall not be kept for longer than is necessary for that purpose or those purposes. For example, once it is clear that there is not going to be an appeal by a student who made an unsuccessful application to the College, steps should be taken to destroy their application.

vi. Shall be processed in accordance with the rights of Data Subjects under the Act. For example, the student has the right to request any data held about them and to request that any errors are corrected.

vii. Shall be protected by appropriate technical and organisational measures which shall be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data. For example, sensitive information should only be accessible to a limited number of staff on a 'need-to-know' basis and if a paper file, locked away, and if stored on computer, password protected.

viii. Shall not be transferred to any 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. For example, a member of staff is giving a lecture at a University in Russia. The College wishes to send the teacher's academic achievements to the University. The teacher's academic records are available publicly and he has no problem with them being sent. In this case, it is unlikely that there would be an issue with adequacy as the teacher has indicated he is happy for the information to be sent and there is little risk of misuse.

Section 3 – Obligations, Rights and Guidelines

Your Obligations

The College and all staff or others who process or use any Personal Data must ensure that they consider and follow the data protection principles at all times. (There are specific exemptions covering: Research - for guidelines see *Appendix D*, References - for guidelines see *Appendix E*, Journalism and certain other specific activities.)

All staff, students and students' parents are responsible for:

- Checking that any information that they provide to the College is both accurate and up to date;
- Informing the College of any changes to information which they have provided, e.g. changes in address;
- Recording any information provided to the College in accordance with this Policy;
- Informing the College of any errors in the information it holds about them;
- Amending any errors in information that is held by the College.

Your Rights

All staff, students and other Data Subjects are given a number of legal rights under the Act. These rights are:

- To prevent data processing for the purposes of Direct Marketing (see Appendix G);
- To ask to have inaccurate data amended;
- To prevent processing that is likely to cause damage or distress to themselves or anyone else; and
- To request access to data held about them by the Data Controller (Subject Access Right)

Subject Access Right
Staff, students and other Data Subjects about whom the College holds or uses data have a legal right to access certain information in accordance with the Act and request a copy of the data in a permanent form. Any person wishing to exercise their right of access formally should be directed to enquire at the College's Reception and complete an access request form (see *Appendix K)*. On each occasion that such an access request is made, the College will make a standard charge of **£10** to cover administrative costs.

Students are entitled to a copy of their Learning Agreement free of charge on request at Reception

Collection of Personal Data

Whenever Personal Data is collected it must be clear to the Data Subject for what purpose(s) the information shall be used. In some cases this will be obvious, for example a student completing an enrolment application form will be aware that the purpose of the form is to make an enrolment decision. However, in other cases it may be less clear, for example if the school wishes to collect parents' email addresses at an opening evening it should make it clear that it is collecting this information for marketing purposes. The designated Data Protection Officer see *Appendix J*) must approve data collection forms (see *Appendix A* for details on collection guidelines).

Processing Personal Data

All staff must take care to use Personal Data held by the College only for the purposes for which they were primarily intended, i.e.:

- Education.
- Student and staff support services.
- Student and staff safety.
- Advertising, marketing, public relations, and general advice service.
- Staff, agent, and contractor administration.
- To keep proper accounts and records.
- The provision of facilities to other groups or organisations.
- Crime prevention and prosecution of offenders.

A complete description of these purposes can be found in *Appendix H*

In particular, addresses and telephone numbers held by the College must not be publicised or used for, or to further, personal, leisure or private business interests.

All local databases containing Personal Data (including those using reference numbers for individuals rather than names) must be registered with and approved by the College's MIS Manager.

Where possible it is recommended that central databases (such as UNIT-e) be used as much as possible to avoid unnecessary duplication of information and to increase data security.

E-mail Usage

The majority of e-mail communications that staff send or receive will be simple transactions regarding College business. Staff should avoid using e-mail to send personal information of a sensitive nature or to express views about any individuals. This is because e-mail is an essentially insecure medium and the sender can have no control over the storage or use of the message after it has been sent. Staff who receive by e-mail, from students or others, information that might be Personal Data or Sensitive Personal Data should print it out and immediately delete the e-mail. (Examples might include any mention of individuals in relation to discipline or performance, family or personal circumstances.) The printed information should then be kept in the appropriate hard copy filing system and be used strictly in accordance with this Policy.

The College reserves the right to monitor the use of its e-mail facilities in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and guidelines in the Student and Staff Handbooks. The College also monitors the use of its internet facilities to ensure they are used within the guidelines in Student and Staff codes of conduct.

Data Storage and Retention

It is the responsibility of the Director – Planning, Systems and Student Services to ensure that centralised records are maintained to meet the needs and reasonable expectations of staff, students, the College, and external bodies such as OFSTED and the ICO. (For details on storage and retention periods see *Appendix C*.)

Security

Each individual must ensure that Personal Data is processed in accordance with a level of security appropriate to the risks represented by the processing and the nature of the Personal Data to be protected. This may mean avoiding use of e-mail and facsimile transmission in favour of confidential post, the use of passwords or encryption for electronic documents and keeping papers under lock and key. The need for security is greater where Sensitive Personal Data is involved.

Particular care must also be taken when taking Personal Data off site. This should include, ensuring that all documents and computers containing personal data are stored securely, personal data stored in electronic form should require a password to access and all passwords for personal electronic devices (such as laptops) which contain personal data must be periodically changed. For further details on security, please see the IT Acceptable Use and Password Policies which are available on our website.

Disclosure of Data

All staff must take care to ensure that Personal Data is neither visible nor accessible to unauthorised persons at any time. This includes taking extra care if working in a public environment such as on a train or in a cafe. Where Personal Data is disclosed to third parties, it must be restricted to only those details that are required for the purpose in hand (see *Appendix B* for details on disclosure guidelines).

Staff should pay particular care to the use of Cedar (Student, Staff and Parent Portal) systems.

Direct Marketing

The Marketing Manager has responsibility for all outgoing mail marketing or telephone marketing and for the content of the College's website(s). No Personal Data must be used or published in these contexts without the specific approval of the Marketing Manager, including for alumni purposes. Any information the College retains for Direct Marketing purposes shall not be passed to any third parties without the express consent of the Data Subjects..
See *Appendix G – Using Personal Data for Direct Marketing* for guidelines on this subject. This applies to marketing targeted at both students aged between 16-18 and adults.

The designated Data Protection Officer (see *Appendix J*) must approve any contracts with third party organisations that involve the processing of Personal Data. It may be necessary for the Data Protection Officer to seek legal guidance.

Breach of the Policy

Should staff not process data in accordance with this Policy. The College and the individual staff member in breach could be liable to criminal prosecution and also civil claims for damages. If any staff are found to have wilfully, recklessly or negligently breached this Policy, they may be suspended from having access to any College data and be subject to action under the Disciplinary Procedure which is available from Moodle.

If any staff member or student believes the College has infringed her/his rights under this Policy, s/he should raise this concern under the College's Grievance or Complaints Procedure respectively which is available from Moodle.

If a member off staff suspects that data security has been breached, including compromised passwords, theft/loss of laptops/devices holding data or any other unauthorised access to the College's data systems they should report this immediately to the Director – Planning, Systems and Student Services.

Monitoring and Review of the Policy

The College will continue to review this Policy every two years to ensure that it is complying with its obligations under the Act. The College remains committed to instilling best practices in our data protection and management policies and procedures. To help the College achieve its stated

objectives, any recommendations that you may have on this Policy are welcomed and should be reported to the Data Protection Officer.

Training

As a College committed to data protection and effective implementation of this Policy and to ensure that best practices are adopted in our management of data, we will provide training to all staff on their obligations under this policy. It is the duty of all staff to attend these training sessions.

Version	Date	Policy Owner	Comments	Approval Route and Date	Provenance	Date of Next Review
1.	January 2011	Julie France	Update			
2.	March 2016	Julie Pryce	Full re-write	SLT approval required	Fundamental revision to include legal requirements	March 2018

Appendix A – Collection Guidelines

Data collection forms must be clearly titled to indicate their purpose(s) and collect only data relevant to those specific purpose(s). All these forms must carry at least the following notice:

Huddersfield New College is fully committed to upholding the principles laid out in the Data Protection Act 1998 and other related legislation. The College's Data Protection Policy is available from the College website.

In addition, if any of the data may be transferred or used in ways that are not immediately obvious this must also be explained to the Data Subject.

Where any forms collect Sensitive Personal Data (other than ethnic origin or disability information used solely for equal opportunities monitoring) the Data Subject's explicit consent to processing must also be obtained using the following formula:

I hereby give permission under the Data Protection Act 1998 for the College to process the data on this form.

For this consent to be valid, the Data Subject must be aware of the purpose(s) behind the processing.

The Data Protection Officer must approve all data collection forms before they are used.

Appendix B – Disclosure Guidelines

For staff in general the following guidelines apply:

Dealing with requests for information:
Under the Act, individuals have the right to access personal data held about them by the College and to request a copy of that information in a permanent form. This 'Subject Access' right includes the right to a description of:

- The Personal Data held;
- The purposes for which the data are being or is to be processed;
- The recipients to whom the data is being or may be disclosed; and
- Any information the college has about the source of the personal data.

When dealing with requests for information ("Subject Access Requests") all staff should refer to the Appendix L 'Subject Access Request Procedure' and ensure that they have reviewed these Disclosure Guidelines. All Subject Access Requests should me made in writing, on the prescribed form (Appendix K) and accompanied by a fee of £10. Where a Subject Access Request is made verbally, the requesting party should be asked to complete the prescribed form. All Subject Access Requests should be notified to the Data Protection Officer before information is disclosed.

Disclosure of Educational Records:

- Where students are living at home with their parents or guardians or where employers or training providers sponsor the training of a student, these stakeholders have a legitimate interest in information about the conduct, progress and attendance of the student concerned (Educational Records). It is therefore College policy to supply Educational Records to these parents, guardians and employers. However, wherever practicable, the student should be made aware in advance of the information to be disclosed. This applies to all full-time daytime students (ie the “main-provision”) irrespective of age.
- No information about students in the Higher Eductaion Provision should normally be given to third- parties without the student’s written permission. If in doubt about the validity of a Subject Access Request, the matter should be referred to the Data Protection Officer.
- No information about students beyond their Educational Records should normally be given to parents, guardians, employers or training providers without that student’s permission. Particular caution should be exercised where parents/guardians have separate interests.
- When disclosing the Educational Records of Data Subjects, care should be taken to avoid the inclusion of any Personal Data about any other Data Subjects. This may include, reference to other students' conduct and progress within the Educational Record of the students subject to the Subject Access Request.
- Disclosure of information to any other outside agency or individual (e.g. police, prospective employer, government or local authority department) without the student’s express written permission may only be made by the Data Protection Officer. Even simple questions such as ‘Is this student attending’ or ‘on such and such a course?’ should not be answered but referred to the appropriate Senior Manager after establishing the information they require and the reasons they require it. Requests that may affect a student’s benefits should be referred to the Data Protection Officer.
- Where the decision is made to disclose information to a third party that information should be disclosed on the basis that the recipient agrees to keep the information confidential and not to use it for any other purpose than that notified to the College as the reason for the request.

- It is essential that before any information is to be disclosed to a party who is not in face-to-face contact, that their identity is properly established. Information may only be given over the telephone or to personal callers after obtaining evidence to establish the true identity of the caller e.g. by using dial-back and by asking security questions based on data held on the College's systems. Where possible such requests should be made in writing before any information is released.
- Information must not be sent outside of the European Economic Area without the express written permission of the Data Subject. Where the decision is made to disclose information to a third party outside the EEA, that information should be disclosed on the basis that the recipient agrees to keep the information confidential and not to use it for any other purpose than that notified to the College as the reason for the request. Written confirmation must be obtained from the third-party before any information is released.
- Enquiries from the media should always be referred, without comment, to the Marketing Manager' or in her/his absence a member of the Senior Leadership Team (**SLT**).
- Do not disclose more information than is necessary and be careful about disclosing information relating to other Data Subjects.
- The College operates a number of CCTV cameras in order to assist with security for members of the College Community and in respect of College property. Signage alerting students, staff and visitors that CCTV monitoring is in action is in place. Release of CCTV images can only be made with authorisation from a member of SLT.

For members of SLT making decisions about appropriate disclosure, the following guidance is provided.

Any Personal Data held by the College should only be disclosed to a third party either:

1. With the permission of the Data Subject.
2. If it is necessary for the purposes of legitimate interests pursued by the third party or the College unless the disclosure is unwarranted in terms of the prejudice to the rights and freedoms or legitimate interests of the Data Subject.
3. Their disclosure is required by law or relates to legal proceedings (in which event the request must be referred to the designated Data Protection Officer (see *Appendix J).*

Most importantly the College holds certain Sensitive Personal Data that should be treated with even more care, and not disclosed even within the College unless certain criteria are met.

Sensitive Personal Data	**Disclosure Guidelines**
The physical or mental health or condition of the Data Subject.	Students are informed on the enrolment form that data regarding disabilities and learning difficulties will be shared with the LSC and other educational agencies. Internally it is necessary that data which may have a *direct* impact on the education of a student - for example, if they are dyslexic - should be provided to those responsible for their education. It is inappropriate to disclose this information to anyone not responsible for the education of the student. It is important that staff responsible for educational visits and other trips have ready access to adequate health records on students in case of emergency.It is inappropriate to disclose any other health information without the express written consent of the Data Subject except in circumstances where permission is unobtainable and disclosure is in the best interests of the Data Subject - for example, a medical emergency where the Data Subject is unconscious and

	disclosure is necessary to facilitate immediate treatment.
His/her religious beliefs or beliefs of a similar nature.	This information is only held for very specific purposes (CES/ACVIC returns) within the College, and disclosure is only appropriate in line with these purposes. Both CES and ACVIC require summative data not information on individuals.
His/her racial or ethnic origin	Students are informed on the enrolment form, and staff on their application form, that we will use this information for equal opportunities monitoring and that this data will also be shared with the LSC and other educational agencies for the same purpose. Even internally to the College this is the only reason for which this data may be disclosed. No other external disclosure can be made without the express written consent of the Data Subject
His/her commission or alleged commission of any offence. Any proceedings for any offence or alleged offence.	This information, in relation to staff, is limited to those people in Senior Leadership, Personnel and Line Managers directly responsible for a person's employment. This information, in relation to students, is limited to Senior Leadership, Director of Student Services, relevant Senior Tutor and Personal Tutor. No other disclosure should be permitted internally or externally without consulting the designated Data Protection Officer (see *Appendix J*).
His/her political opinions. His/her sexual life. Details of trade union membership.	The College does not collect data regarding staff/student political opinions or sexual life. The College does not collect union membership details from teaching staff. Some support staff elect to pay union levies through payroll. This information is held within payroll only. It is College policy that this information is not disclosed beyond this function.

In all cases best practice is to consider whether you would want similar data the College holds about you to be disclosed in similar circumstances, and consider if there are alternative courses of action that could be taken where Sensitive Personal Data is not disclosed. In some cases it may be possible to anonymise the data before disclosure. For example in certain circumstances we might disclose that we have a certain number of disabled staff, but it would be inappropriate to disclose any other information that may identify them individually.

It is recommended that if you are in doubt you obtain advice from the designated Data Protection Officer (see *Appendix J)*

In all circumstances your first thought should be 'what is in the best interests of the Data Subject?'

Appendix C – Retention Guidelines

Staff Data

Type of Data	Suggested Retention Period	Reason
Personnel files, including health records, risk assessments and appraisals	Six years from the end of employment	Reasonable period of time within which to provide references
Pension Details	72 years from birth or five years after retirement, whichever is longer	
Application forms	Six to twelve months	In case a complaint is made or claim brought to the College concerning the process.
Redundancy facts	12 years from date of redundancy	In case a complaint is made or claim brought to the College concerning the process.
Income tax and NI	Three years from the end of the financial year to which they relate	Income Tax [Employment] Regulations 1993
Maternity pay		Statutory Maternity Pay [General] Regulations 1986
Statutory sick pay		Statutory Sick Pay [General] Regulations 1982
Wages and salaries	Six years	Taxes Management Act 1970
Accident books	Four years after date of last entry	RIDDOR 1995
Health records where termination of employment is related to, and Medical records relating to, Control of Substances Hazardous to Health	40 years from date of last entry	COSHH 1994, 1998
Health records where termination of employment is due to asbestos-related illness	50 years	Control of Asbestos at work Regulations 1987
Disciplinary records	Details of any disciplinary matters will be removed from staff files after a length of time recorded at the disciplinary hearing **but** a copy of the lapsed warning will be kept on file as a part of an accurate record of the employment relationship.	

Student Data

Type of Data	Suggested Retention Period	Reason
Achievement records	Ten Years	Record of grades may be required throughout career
Courses studied Start and end dates	Ten Years	Reasonable period of time within which to provide references

Tutor references		
Enrolment forms Amendment forms Registers Attendance books and other contact records, e.g. distance learning	Three years after completion of course	Audit requirements Inspection
Student disciplinary records Welfare forms	Three years after completion of course	Possible litigation Inspection
Coursework marks Student concern records Risk assessments	One year after end of course	Appeals Inspection
Student Work	As required by relevant awarding bodies. In addition see guidelines issued by the Deputy Principal re: Inspection	Internal and external verification Student appeals Internal and external inspection
Other student information e.g. Progress notes, other course or student administration records	Either academic year or duration of course as necessary	Not required after course completion
Reasons for EMA/ALG non-payment	Three years after the student completes course	Audit requirements

General Data

Type of Data	**Suggested Retention Period**	**Reason**
Professional Advice Records e.g. Careers, Personnel	Kept as long as is necessary to open and process a case and for five years from case closure	Necessary for processing and potential follow on queries
CCTV footage	30 days (unless there are any incidents which are kept securely until resolved)	Security of staff, students, visitors and property
Internet Monitoring Records	3 years	Ensuring facilities are used within guidelines

If you wish to retain Personal Data other than in accordance with these guidelines, seek guidance from the College's designated Data Protection Officer (see *Appendix I*).

The Data Protection Act 1998 specifies that we should not keep Personal Data for longer than is necessary for our stated purposes (see *Appendix H – Notified Purposes*). The above is designed to help achieve this. Equally, Data Subjects have the right to expect us to keep records for these necessary periods in case they should require access to them. Once the document has been kept for the maximum time it should be destroyed, with the same care taken to avoid accidental disclosure of the information. Where practicable, shredding is recommended as the most appropriate and secure way of destroying paper documents and this is the standard method of destruction currently used by the College.

It should be noted that where any documents are required for investigation by relevant external bodies they may be kept longer than indicated in the above guidelines.

Appendix D – Research Exemptions

It should be noted that where Personal Data is collected for research purposes it is exempt from certain aspects of the Data Protection Act 1998.

Conditions of the Exemption
Specifically, Personal Data collected for research purposes must not be used in forming any decisions about a particular individual, and must not be used in any way that will, or is likely to, cause distress to any Data Subject.

If you are collecting Personal Data for research within these parameters the following exemptions apply:

- Processing the Personal Data for additional research purposes (other than those notified to the Data Subject on collection is permitted.
- Personal Data processed only for research purposes may be kept indefinitely.
- Personal Data processed only for research purposes () and which is not made available in any form that identifies Data Subjects is exempt from the Subject Access Riight

Therefore it is recommended that when Personal Data is collected for research purposes:

- The Data Subject should be informed of the purposes for which the data is being collected.
- Any data collection forms should make clear that the data will be used only for research, what the research is for, and that any published results will be anonymised.

All other provisions of the Act apply, notably the requirement for adequate security when processing Personal Data whether or not within the above parameters.

Appendix E – Student Reference Guidelines

1 Introduction

There is no specific legal obligation on the College to provide a reference for an employee or former employee as there is not a requirement in the contract of employment, but the College could be subject to a claim for discrimination if it refused to provide a reference for reasons relating to sex, race, disability etc (See Section 2.3 below). Nevertheless, as a good employer, it is standard practice to give a reference to an employee upon request. It is also College policy to give references for students on request.

2 Accuracy of Student References

Staff should refer to the UCAS Training Pack for further information

2.1 Responsibility to Students

It is the duty of the reference writer to exercise reasonable care and skill in providing a reference. The writer should take reasonable steps to:

- Ascertain that the information on which the reference is based is factually correct. Even if the reference writer honestly believes the inaccurate statements to be true, he/she may still be negligent if reasonable steps have not been taken to check the veracity of statements.

- If the writer chooses to express opinions about the subject of the reference, they should ensure that the opinions expressed are reasonable in the circumstances and can be justified. Opinions are, by their very nature, subjective but they must be arrived at reasonably. The person expressing the opinion should always ask whether, if called upon to do so, he/she could justify why he/she holds those opinions – i.e. whether the opinion has a proper basis in fact. Statements of opinion should not be presented as statements of fact.

- There is nothing to prevent the reference writer from showing the subject the reference before submitting it. Their consent will ensure compliance with the Act.

- Create a fair impression overall. This might mean putting certain factual matters into context where not to do so would create a misleading impression. Having checked the factual accuracy of statements and the reasonableness of opinions contained in the reference, the writer should "stand back" and ensure that the effect of the whole reference is fair and not misleading.

A reference writer who is negligent in the above respects will render the College liable for any loss, which the student incurs as a direct result of inaccurate statements, opinions or impressions.

Where the person providing the reference has limited knowledge of the subject, this should be clearly stated.

In appropriate cases the College may make the provision of a reference conditional upon a disclaimer of liability to the subject and to the recipient.

Whilst it may sometimes be tempting to provide a reference that portrays the student in a better light than is justified this should not be done since a reference which is unduly favourable could potentially leave the College vulnerable to a claim for damages from the recipient of the reference.

2.2 "In Confidence"

Many references are written and received "in confidence". If, however, there is a claim for damages the reference may have to be disclosed. It should also be noted that references received and held on file would have to be disclosed in the event of a subject access request by the Data Subject. Reference writers need to be aware of this when drafting references.

2.3 Equal Opportunities and References

It is unlawful to discriminate on grounds of race, sex, disability, sexual orientation, religion or religious belief, part-time status, fixed term employment contract status or trade union membership or activity. It is specifically unlawful to instruct, procure, induce, comply with, or knowingly aid, an act of unlawful discrimination.

In giving and acting upon references, care should be taken to avoid overt or covert, intentional or unintentional acts of unlawful discrimination. This is particularly the case where opinions not based on any objective evidence are sought or offered on the suitability of applicants. Opinions should, therefore, be capable of being backed up by objective evidence.

Particular care should be exercised when acting on references received from referees where it appears that applicants may have experienced difficulties arising from their race, sex, marital status, disability, age, sexual orientation, trade union membership and activity, political or religious belief, or unrelated criminal convictions.

3 Giving Student References

When replying to a request for a general student reference, if specific questions are asked, the College will decide whether to answer none of them, all of them or to leave out questions unanswered.

As a general rule, check all references written to ensure that the content is accurate, justified, true and not misleading. State the facts and opinions that can be substantiated – "if in doubt, leave it out". Speculative statements should also be avoided. Consider showing the subject the reference before releasing it.

Reply promptly to reference requests, as the person's future may be dependent on the reference.

Disclosure of References

3.1 If there is a request to see the reference then it should be considered, bearing in mind that the reference may have to be disclosed at the request of the referee to the recipient or during legal proceedings.

3.2 Open References

Open references are those not addressed to a specific person or for a specific job– i.e. "To whom it may concern". They are general statements about an individual that can be re-used in a variety of different circumstances. As they do not fall within the remit of "qualified privilege", libel claims are possible.

As a duty to take reasonable care applies equally to open references, they should be written with caution. They should also be dated so that they cannot be used years after they were written when circumstances may have changed.

3.3 Telephone References

Requests for telephone references should be approached with caution and avoided.

Only Senior Leaders (or designated staff) have the authority to give telephone references, if they cannot avoid giving a telephone reference then they should abide by the following:

- Do not say anything that you would not be prepared to put in a written reference.
- If the person requesting the reference is unknown, ask for their workplace telephone number then call them back to ensure you are speaking to the right person at the right organisation.
- Do not be hurried or harassed into replying.
- Reserve the right not to answer specific questions but be as helpful as possible.
- Take notes of the questions asked and the answers given.
- Follow up in writing with a summary of the facts discussed on the telephone.

3.4 Provider of Written Student References

- Current and Past Students

  References should be written by the relevant Progress Tutor and forwarded to the relevant Student Support Manager/UCAS co-ordinator for checking and then to the Principal for signature.

Appendix F – Staff Reference Guidelines

Current and Past Staff

All requests for staff references should be written by the relevant member of the SLT (or relevant delegated manager) and then forwarded to the Principal for approval and signature.

Appendix G – Using Personal Data for Direct Marketing

Under the Data Protection Act 1998 (Section 11) an individual has the express right to object to the use of their Personal Data for direct marketing purposes. 'Direct Marketing' is defined in the Act as meaning the communication of any advertising or marketing material that is directed to particular individuals.

It is obviously best practice for the direct marketer to inform the Data Subject of this right, and the Information Commissioner expects this. For this reason there are 'opt-out' boxes on Application and Enrolment forms as filled in by students allowing them to indicate their desire to exercise this right. **If we are Direct Marketing to an individual who has exercised this right we are in breach of the Act.**

Any information we retain for the purpose of Direct Marketing will be retained solely for marketing and promotion of the College and shall not be passed to any third parties without first gaining the express consent of that individual.

If an individual has exercised this right, the only marketing material we could send them would be in response to a specific request. For example a student has ticked the 'opt-out' box on their enrolment form, and subsequently requests a part-time prospectus. In this case we could send a part-time prospectus, but no other material.

Any Direct Marketing that takes place must include a note stating that the marketing is from Huddersfield New College and that individuals have a right to prevent processing for Direct Marketing purposes. All marketing must also have a simple mechanism which allows the recipient to opt-out of receiving further marketing if they so wish, for example, a return email address.

The College will comply with any request to stop processing for Direct Marketing purposes within a reasonable period of time and in any event before the end of 28 days from the date of request.

Obviously, in order to fulfil our obligations to Data Subjects we must maintain up-to-date databases that allow us to remove or otherwise exclude individuals who have exercised their right to prevent processing. The UNIT-e database of student data is maintained as the most accurate record of students' wishes in this regard. Student Services hold the current list of students who have 'opted out' of marketing/promotion.

Appendix H– Notified Purposes

The following is the list of purposes for processing Personal Data that the College has notified to the Information Commissioner.

- **Staff, agent, and contractor administration -** The administration of prospective, current and past staff including self employed, contract personnel, temporary staff or volunteer workers. Administration of non-College staff contracted to provide services on behalf of the College. Planning and management of Data Controller's workload or business activity. Occupational health service. Administration of agents or other intermediaries. Pensions administration. Disciplinary matters, employment tribunals, etc. staff training.
- **Advertising, marketing, public relations, and general advice service -** The identification of recipients for College services and administration of promotional campaigns. The advertising and promotion of the College and its services including by Direct Marketing means. The advertisement and provision of general advice to members of the public about College services. Fundraising for the College and other organisations.
- **Student and staff safety –** To ensure that adequate records, such as medical records and other personal information is kept to ensure both the physical and mental well-being of both the students and staff.
- **Accounts and records -** Keeping accounts related to any business or other activity carried on by the Data Controller. Deciding whether to accept any person as a customer or supplier. Keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made and/or services provided by or to the Data Controller in respect of those transactions. For the purpose of making financial or management forecasts to assist the Data Controller in the conduct of any such business or activity. The administration of supplier records relating to goods, orders, services and/or accounts provided to the College.
- **Education -** The provision of education or training as a primary function or as a business activity. Administration of education and training (e.g. admissions administration, monitoring, calculation and publication of exam results, provision of references, etc.). Provision of education and training (e.g. planning and control of curricula and exams, commissioning, validating and producing educational materials, work experience placements, etc.). Liaison with education, training establishments, employers – past, current and potential. Preparations of Department for Education and Skills, Learning and Skills Council and European Social Fund returns. Administration of student awards and fees (e.g. access funds, Adult Learning Grant, Bursaries/Free School Meals, charges for equipment &materials, re-sits etc.). Administration of external visits and residential courses.
- **Student and staff support services -** Administration and provision of library services (including membership records, loan/hire records, information and databank administration). Administration and provision of a student card. Administration and provision of welfare and pastoral services. Careers guidance.
- **Crime prevention and prosecution of offenders -** Crime prevention/detection and the apprehension/prosecution of offenders. Security, including use of CCTV for monitoring and collecting sound and/or visual images for the purpose of maintaining the security of premises, preventing crime and investigating crime.
- **Provision of facilities to other groups, organisations or people.**
- **Publication of College magazine.**

Appendix I – Privacy Notice to be included on the student learning agreement

Version 1 – Published March 2016.

This privacy notice is issued by the Skills Funding Agency (SFA) on behalf of the Secretary of State for Business Innovation and Skills to inform learners of how their personal information will be used for statutory and other legitimate purposes by:

1. the SFA, an executive agency of the Department of Business Innovation and Skills (BIS)
2. BIS
3. the Department for Education (DfE), including the Education Funding Agency
4. any successor bodies to these organisations
5. by other bodies with whom data is shared by the SFA

BIS and the DfE (largely for learners age 16-18) are data controllers of this information.
Providers should ensure that all learners have seen the privacy notice as part of their enrolment processes.

Privacy Notice

How We Use Your Personal Information
The personal information you provide is passed to the Skills Funding Agency, and the Department for Business, Innovation and Skills. Where necessary it is also shared with the Department for Education, including the Education Funding Agency.

The information is used for the exercise of functions of these government departments and to meet statutory responsibilities, including under the Apprenticeships, Skills, Children and Learning Act 2009, and to create and maintain a unique learner number (ULN) and a personal learning record (PLR). The information you provide may be shared with other organisations for education, training, employment and well-being related purposes, including for research.

You may be contacted after you have completed your programme of learning to establish whether you have entered employment or gone onto further training or education.

You may be contacted by the English European Social Fund (ESF) Managing Authority, or its agents, to carry out research and evaluation to inform the effectiveness of the programme.

Further information about use of and access to your personal data, and details of organisations with whom we regularly share data are available at:
https://www.gov.uk/government/publications/sfa-privacy-notice

Appendix J - Further information and contact details

Staff who have queries on data protection issues should refer to their line manager. Managers may then if necessary approach the Director to SLT – Planning, Systems and Student Services, who is the College's designated Data Protection Officer.

Students should refer in the first place to Student Services for advice and guidance on any problems or queries regarding data protection.

For external guidance, individuals can contact the ICO on 0303 123 1113 or 01625 545745 or visit the website at: http://www.ico.gov.uk/

Appendix K – Subject Access Request Form

Name:	
Staff/Student/Other: (delete as appropriate)	
Student/Staff PIN	
Please provide below details of the information you require and a address:	
Date £10 charge collected:	
Date information to be provided by: (40 days after charge collected)	
Signature:	
Date:	
Staff signature:	

Personal Data provided on this form will be used solely for the purposes of identifying the Data Subject making the request and complying with their request under the Data Protection Act 1998.

Information for staff processing this form: See *Appendix L* for guidance and contact the Data Protection Officer if you have any questions.

Appendix L:

Subject Access Request Procedure:

1) Obtain information to establish the identity of the requesting party. Are you confident that the person making the subject access request is who they say they are? You may want to consider the following question:

- It is essential that you satisfy yourself of the true identity of the party requesting the information.
- Ask yourself, who am I dealing with? What measures can I take to establish their identity?
- Ask the requesting party to confirm information that you hold on the Data subject

↓

2) Inform the Data Protection Officer and identify the information that you may reasonably require to provide the requesting party with the information they want.

↓

3) Establish the fee that is to be charged to provide the requesting party with the information and inform them before taking further steps.

- The College will make a standard charge of £10 to cover the administrative costs of subject access requests.
- Where educational records such as examination scripts are requested, the college may exercise its discretion to charge more for the costs involved (the limits being set by the ICO are available on their website)

↓

4) If no Personal Data is held about the requesting party you must inform them.

↓

5) You must not make any changes to the records as a result of receiving the request.

↓

6) If the information to be disclosed contains Personal Data of third parties then this must not be disclosed unless you have the consent of that third party or it is reasonable to supply the information without their consent.

- Where the information of third parties is not to be disclosed, ensure that you have undertaken sufficient editing or redacting

7) If the information requested is covered by an exemption then you are not required to reveal the information. If all of the information subject to the request is covered by an exemption then you can reply to the requesting party stating that you do not hold any of their Personal Data. The applicable exemptions are:

- Crime prevention and detection;
- When engaged in negotiations with the requester;
- Management forecasts;
- Confidential references given by the College;
- Information used for research, historical and statistical purposes (see Appendix D);
- Information which is covered by legal professional privilege.

8) Prepare the Response.

- If the information requested is not covered by an exemption, then the information should be supplied to the requesting party in a permanent form.
- The response must be sent to the requesting party within **40 days** of receipt of request.