Policy Name	**Data Protection Policy**
Policy Version	1.1
Department / Area	College Wide
Created By	Vice Principal Finance and Resources
Amended By	Vice Principal Finance and Resources
Last Updated	17 August 2016
Approved by SLT	XX XXXXX 2016
Next Review	17 August 2017
Equality Impact Assessed	Yes – Date XXXXX
Document REF	HR016
Category	Public
Covers	Staff / Student / Both

European Union
European
Social Fund

Contents

1. Purpose and Scope

The 1998 Data Protection Act was passed by Parliament to control the way information is processed and to give legal rights to people who have information stored about them. Telford College of Arts and Technology is committed to protecting the privacy of individuals in accordance with the Data Protection Act 1998 (DPA). The College needs to process certain personal data about employees, learners and third parties in order to monitor performance, achievements, fulfil its purpose and to meet its legal obligations to funding bodies and the government. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. Any personal information must be collected and dealt with appropriately whether it is collected on paper, entered electronically or stored in a computer database. To do this, the College must comply with the Data Protection Principles as set out in the Data Protection Act.

In summary the principles state that information should be:

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

The College will not release staff or learner data to third parties except to relevant statutory bodies. In all other circumstances the College will obtain the consent of the individuals concerned before releasing personal data.

This policy is published on the College website – www.tcat.ac.uk and is subject to a review annually.

2. Data Controller and College responsibilities

The Corporation is responsible for the oversight and implementation of this policy. It will be the responsibility of the Principal and the Senior Leadership Team to ensure compliance with the policy and for communicating the policy to all staff.

The College's designated Data Controller is the Vice Principal Finance and Resources who has the operational responsibility, on behalf of the college to ensure:

- The College's Policy and Codes of Practice are appropriate for the types of personal data being processed
- The College maintains an up-to-date notification of its use of personal data with the Data Protection Commissioner

- The 'Data Controller' determines the purposes and the manner in which personal data is to be processed. This may be an individual or an organisation, and the processing may be carried out jointly or in common with other persons.

The Vice Principal Finance and resources is supported in their duties by the Director of Quality and HE who manages the day to day data protection requests and queries.

However, there are other designated senior managers within the College organisational structure that have specialist areas of responsibility that are regularly subject to requirements of the Data Protection Act:

- All members of the College Senior Leadership Team
- Director of MIS
- Head of Learner Services
- Learning Support Manager
- Network Manager
- College Accountant

Any in-house queries with regard to DPA should be addressed initially to either the Director of Quality and HE or the Vice Principal Finance and Resources. They maintain an MIS DP Tracking sheet on behalf of the college ensuring the duties of the DPA are met.

This policy does not form part of the formal staff contract of employment, but it is a condition of employment that staff abide by the rules and policies made by the College. Any breach of the policy could, therefore, result in disciplinary proceedings. It may also result in a personal liability for the individual staff member.

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

<u>Employee Information – All Employees are responsible for:</u>

- ✓ Checking that any information they provide to the College in connection with their employment is accurate and up-to-date.
- ✓ Informing the College of any errors or changes to information held. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

<u>Employee Responsibilities - All Employees of the College are expected to:</u>

- ✓ Attend the college Data Protection Training in their compulsory induction or as part of the annual sessions
- ✓ Read and understand this policy document
- ✓ Be aware of and abide by the Data Protection Principles
- ✓ Understand what is meant by "sensitive personal data" and know how to handle such data
- ✓ Contact the Vice Principal Finance and Resources, or the Director of Quality and HE for advice/support if they are unclear about the rules they must follow in order to comply with the DPA.

Learner Information – All employees:

- ✓ MUST adhere to the staff guidelines in Appendix 1 regarding processing learner data.
- ✓ Failure to comply with the data protection policy, college procedures or staff guidelines could result in disciplinary action.
- ✓ Refer to the Data Retention Policy for guidelines on the retention and destruction of personal data.

3. Learner Obligations

Learners must ensure that all personal data provided to the college is accurate and up-to-date. They must ensure that changes to their personal details (e.g. address/contact details) are notified to learner services and their personal tutor.

Learners who use the college computer facilities may, from time to time, process personal data. If they do they must notify the data controller. Any learner who requires further clarification about this should contact the facilities supervisor.

4. Notification of Data Held and Processed

All staff, Learners 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 Data Protection Act 1998

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 and/or failure to adhere to the requirements set out below will usually be a disciplinary matter, and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member.

Personal information should be:

- Kept securely in one of the managed college systems
- Kept in a locked filing cabinet, or a locked drawer, or maintained in a locked office environment
- Should only be kept as an electronic record within the college's internal networks and drives.

Personal information should not be:

- Taken offsite if it's considered 'sensitive', or if it contains payroll information, addresses of learners and staff, disciplinary or appraisal records or bank account

details. Exceptions to this may only be with the explicit agreement of the college Data Controller.

- Emailed electronically to any external agencies or email addresses unless permission given under a data sharing agreement or it has been recorded in the MIS DP Tracking process approved by the Vice Principal Finance and Resources.
- Taken off site on portable media unless authorised and essential. Where approved all of the files on the portable media must be encrypted and password protected.
- Processed at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the Data Controller must be obtained, and all the security guidelines given in this document must still be followed.

Where data is stored on portable electronic devices or removable media it is the responsibility of the individual member of staff who operates the equipment to ensure it is kept safe and not left unattended.

5. College commitment to protecting data

Our data protection policy sets out our commitment to protect the personal data stored in the college and how we implement that commitment with regards to the collection and use of personal data.

We are committed to:

- Ensuring that we comply with the data protection principles
- Meeting our legal obligations as laid down by the Data Protection Act 1998
- Minimising the amount of personal data we process from our learners, and only do so to meet operational needs or fulfil government funding requirements
- Take due care and attention to ensure that personal data is up to date and accurate
- Establishing appropriate retention periods for personal data
- Ensuring we have clear processes in place so that data subjects' rights can be responded to in accordance with the duties placed on us
- Providing adequate security measures to protect personal data
- Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues
- Ensuring that all staff are made aware of good practice in data protection
- Give all staff access to the Data Protection Training on an annual basis
- Ensuring that everyone handling personal data knows the requirements

The Data Controller is the primary contact to the Information Commissioner and is responsible for ensuring provision of suitable DPA advisory, training and awareness services and DPA request handling.

This document should be read in accordance with the Data Retention Policy which can be found at www.XXXXXXX

6. Governance

This policy has been approved by the Senior Leadership Team (SLT) and any breach will be taken seriously and may result in more formal action including dismissal or expulsion. It will be reviewed annually.

If anyone considers that the policy has not been followed, they should raise the matter with the Data Controller.

7. Rights to Access Personal data

Employees, learners and other users of the College (data subjects) have the right to access any personal data which is kept about them.

The College is committed to facilitating access by data subjects to their personal data. All data subjects will be expected to complete a "Subject Access request form" (see appendix 2) requests to access personal data will be handled according to the DPA.

Process for Data subject requests:

- For staff members of the College if they submit The Subject Access Request Form via their own College login and email account no further proof of ID will be required.
- For non-college staff (learners, employers, external agencies or members of the public) they must submit the Subject Access request form with proof of ID which establishes that they are the data subject (or where the application is made by a third party on behalf of the data subject, which establishes the third party's identity, that of the data subject and a form of authority signed by the data subject must be provided).

The fee for a subject access request is £10 per day. However this fee only applies if the request is deemed to take more than half a day to process. The College retains its own discretion to waive this fee should they feel it appropriate.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a completed and signed "Subject Access request form".

8. 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 learner onto any course, and a condition of employment for staff. This may include information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974.

Some jobs or courses may bring staff or learners into contact with children, including young people between the ages of 16 and 18. The college has a duty under the Children's Act 1989 and other enactments to ensure that staff and learners are suitable for job roles and for the courses offered. The college also has a duty of care to all staff and learners and must

therefore make sure that those employees and others who use the college facilities do not pose a threat or danger to others. Therefore, all prospective staff and learners will be asked to consent to their data being processed when an offer of employment or a course offer is made. A refusal to sign such a form may result in the offer being withdrawn.

9. Processing Sensitive Information

Sometimes it is necessary to process personal information about criminal convictions, race, gender and family details. This may be to ensure that the college is a safe place for everyone, or to operate other college policies such as the Sick Pay Policy or Equal Opportunities Policy. The college may also ask for information about particular health needs, such as allergies to particular forms of medication, conditions such as asthma, diabetes or disabilities or any other medical conditions.

The college will only use the information in the health and safety of the individual or to fulfil the requirements of the college's commitment to the use of the Disability symbol, but will need consent to process this information, for example, in the event of a medical emergency. As this information is considered sensitive, and it is recognised that the processing of it may cause concern or distress to individuals, staff and learners will be asked to give express consent for the college to do this. Offers of employment or offers of a course placement may be withdrawn if an individual refuses to consent to this, without good reason.

10. Photography and Filming Consent

When undertaking photography or filming on college premises "*photography/filing taking place"* signs MUST be clearly displayed in the surrounding area.

If learners are over 18 years you must ask them to complete a photo consent form. Photography/filming MUST NOT take place until the learners have consented in writing.

If learners are under 18 years Parental/Guardian consent must be sought when the images being taken are for non-course related activities. In these circumstances photography/filming MUST NOT take place until Parental/Guardian consent in writing has been received.

If the images are to be used on the college website, college social media or for other marketing purposes then learner/parental/guardian consent must be obtained prior to the images being used. You must ensure that all learners are aware of why you are taking their image and how it will be used.

All consent forms will be stored in either the Course Team Files or with the Marketing Department.

Images which are taken using a member of staffs' personal device MUST be transferred onto the college system and deleted from the personal device immediately after transferring. Storing images on a personal device will be in breach of this policy and will usually be a disciplinary matter, and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member.

11. Examination Marks

Learners are entitled to information about their marks for both coursework and examinations. This is within the provisions of the Act relating to the release of data. 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 are returned to the college.

12. Conclusion

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

Appendix 1 - Staff Guidelines for Processing Learner Data

College staff process data about learners on a day to day basis. This includes completing enrolment forms, marking registers, marking assignments, writing reports or references, in cases of pastoral support or during Head on Duty incidents.
The College has a duty to ensure during the enrolment process all learners understand how their data will be shared and used by the college. All staff must understand the rules set out on the enrolment forms and the printed learning agreements which are designed to protect learners.

Learner information that staff may come into contact with includes:

- General personal details such as name, address, date of birth, photo ID
- Data relating to class attendance, course work marks and grades and associated comments
- ProMonitor and safeguarding information about attendance, behaviour and discipline.

Information classified as sensitive must not be shared without approval by a designated senior manager. Information could include:

- physical disabilities
- learning difficulties or mental health
- sex life
- political or religious views
- trade union membership
- ethnicity.

All staff have a duty to make sure that they comply with the Data Protection principles, which are set out in the College Data Protection Policy.

Staff must not disclose personal data to any student without authorisation or agreement from the data controller.

All data sharing requests must be made in writing to the Director of Quality and HE.

Staff shall not disclose personal or sensitive data to any other staff member, or external agency, except with the authorisation or agreement of the data controller or approval by a designated senior manager with authority.

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

- *Do you really need to record the information?*
- *Is the information 'sensitive'?*

- *If it is sensitive, do you have the data subject's express consent to record it?*
- *If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the learner to collect and retain the data?*

- *Has the student been told that this type of data will be processed?*
- *Are you authorised to collect/store/process the data?*
- *Are you sure that the data is secure?*

Appendix 2 - College Subject Access Request Form

I ……..(name) wish to have access to (delete as appropriate)

1. All of the data that the college currently holds about me, either as part of an automated system or part of a relevant filing system;

   Or

2. Data that the 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
- ☐ Information regarding previous criminal convictions
- ☐ Race, gender or family details
- ☐ Personal details including name, address, date of birth etc.
- ☐ Statements of opinions relating to my abilities or performance
- ☐ Other information

Please tick as appropriate

I understand that I may have to pay a fee of £10

Signed ……..

Date ……