DATA PROTECTION POLICY

This policy is available on-line at: www.tynecoast.ac.uk

- We will consider any request for this policy to be made available in an alternative format or language. Please note that the College may charge for this. Please contact: Director of IT
- We review our policies regularly to update them and to ensure that they are accessible and fair to all. We welcome suggestions for improving the accessibility or fairness of this policy.

Approved by:	Version:	Issue Date:	Review Date:	Contact Person:
Board	v.13	November 2024	November 2027	Director of IT

DATA PROTECTION POLICY

1. Policy Statement

Tyne Coast College is required to retain certain information about its employees, students and other persons in order to facilitate the monitoring of performance, achievements, and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

To comply with the law, information stored in files (either paper based or electronically including e-mail, internet, intranet or portable storage devices) must be collected and used fairly, stored and disposed of safely, and not disclosed to any other person unlawfully.

All data processed by the College will be done so in keeping with the principals of the UK data protection legislation , in particular data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and only used or those purposes.

c) adequate, relevant and limited to what is necessary for the purposes for which it was obtained;

d) accurate and kept up to date; every reasonable step must be taken to ensure that data which is inaccurate is erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary; data may be stored for longer periods for archiving purposes or statistical purposes subject to appropriate safeguards; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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

2. Scope

This policy applies to all members of the college community (staff (including agency workers), governors, students, contractors/suppliers and members of the public).

This policy does not form part of the formal staff contract of employment nor of the student contract with the college, but it is a condition of both contracts that college

regulations and policies must be adhered to. A failure to follow the policy may result in disciplinary proceedings.

Any members of staff or learners who consider that the policy has not been followed in respect of personal data about themselves or about other data subjects should raise the matter with the Data Protection Officer initially (students may wish to do this through their lecturer or course tutor). If the matter is not resolved to their satisfaction they have right to lodge a complaint with the Information Commissioners Office (ICO) who are the UK data protection regulator.

3. **Legislation**

- Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Education Act 2002
- EU General Data Protection Regulation 2018
- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019

4. **Responsibilities**

4.1. All college staff have responsibility for

4.1.1. Checking that data they provide to the college in connection with their employment is accurate and up to date.

4.1.2. Informing the college of changes to information which they have provided, e.g. change of address.

4.1.3. Checking the data that the college will send to them from time to time, which gives details of information kept and processed about them.

4.1.4. Informing the college of any errors or changes. The college cannot be held responsible for any errors which staff members have had the opportunity to correct.

If and when, as part of their responsibilities, staff collect information about other people, (i.e. about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances) they need to follow the data collection principles

4.2. The Data Protection Officer.

The college as a Body Corporate is the Data Controller under the Act and the Board of Governors is therefore ultimately responsible for ensuring implementation of the Act. However, the designated Data Protection Officer will deal with day to day matters.

The Director of IT, Craig Scott, is the designated Data Protection Officer

5. Data Processing

5.1. Types of information we process

We process information relevant to the above reasons/purposes. This may include:

- personal details
- family details
- lifestyle and social circumstances
- financial details
- education and employment details
- student records
- visual images, personal appearance and behaviour
- goods or services provided

We also process special category data that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs
- trade union membership
- offences and alleged offences
- criminal proceedings, outcomes and sentences

5.2. Who the information is processed about

We process personal information about:

- our students
- employees
- current, past and prospective employers
- professional advisers, consultants
- business contacts
- welfare and pastoral professionals
- complainants, enquirers
- persons who may be the subject of an enquiry
- suppliers and service providers
- individuals captured by CCTV images

5.3. Who the information may be shared with

We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act 2018 (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Where necessary or required we share information with:

- family, associates and representatives of the person whose personal data we are processing
- professional advisers
- current, past or prospective employers
- educators and examining bodies
- trade, employer and professional organisations
- UCAS
- trade unions and staff associations
- voluntary and charitable organisations
- healthcare, social and welfare organisations
- suppliers
- financial organisations
- survey and research organisations
- persons making an enquiry or complaint
- careers service
- press and the media
- local and central government
- security organisations
- police forces, prison and probation services, courts and tribunals
- suppliers and service providers

5.4. Transfers

It may sometimes be necessary to transfer personal information overseas. When this is needed information may be transferred to countries or territories around the world. Any transfers made will be in full compliance with all aspects of the DPA

6. Legal Basis for Processing

We will process data

- Where we have obtained consent from the individual, in the case of students this will usually be obtained at point of enquiry, application, or enrolment
- Where we have contractual obligations to process data. Examples include, but are not limited to, contracts with government agencies such as the Education Skills Funding Agency, contracts with employers to deliver training to their employees, and contracts with students (learning agreements) to deliver education and training.
- Where processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- Where we have other legitimate reasons which are consistent with the delivery of education or training, and related support, advice and guidance to current or past students or employees
- Where the processing is necessary to ensure the health & wellbeing of current or past students or employees.
- Where we have other legal obligations to process the data

7. Actions to Implement and Develop Policy

7.1. Information Security

All staff have responsibility for ensuring that:

- Any personal data which they hold is stored and disposed of securely.
- Personal information is not disclosed orally, in writing, accidentally, or otherwise to any unauthorised third party

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

Personal information should be stored securely, usually this means

- In a locked office, or
- In a locked filing cabinet, or
- In a locked drawer, or
- If it is computerised, be password protected, or
- If it is kept on portable storage (i.e. USB, laptop etc..) be encrypted and itself kept securely

The Information Security Policy should be consulted for guidance on storage, transmission, encryption and disposal of data owned by the college.

7.2. Unauthorised Access

Any member of staff or student who deliberately gains or attempts to gain unauthorised access to personal data on any data subject or discloses such data to any third party may be disciplined in accordance with college procedures and where relevant report to law enforcement

7.3. Student Obligations

Students must ensure that all personal data provided to the college are accurate and up to date. Students must ensure that changes of address, etc, are notified to MIS, admin office or Dr Winterbottom Hall as appropriate.

Students who use the college facilities may wish, from time to time, to process personal data. If they do they must obtain the prior permission of their course tutor.

7.4. Rights of Access to Information

Staff, students and other data subjects have the right of access to any personal data that are being kept about them either on computer or in certain other files. Any person who wishes to exercise this right should complete the college “Data Subject Access Request” form. Forms are available from the Intranet

The college aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month unless the requests are complex, or numerous. In such cases, the reason for delay will be explained in writing to the data subject making the request.

In the case of requests which are manifestly unfounded or excessive we may refuse to respond, or choose to charge a fee to cover our costs (staff time & materials) in relation to preparation of our response.

7.5. Exemptions

GDPR contains exemptions to allow disclosure of data to safeguard

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters

Requests to disclose data on the grounds of the above exemptions should be submitted to the Data Protection Officer using the “Data Disclosure Request” form (available from the college intranet)

No data should be released until the request form has been appropriately processed and release agreed by either the Data Protection Officer, or the COO or CEO.

7.6. Emergency Situations

In the event that we have reason to believe there is an imminent danger of death or injury to a person, or where a crime is in progress, it may be necessary to disclose personal data to the Police or other emergency services urgently.

In these cases, it is permissible for any staff member to provide this data to the emergency services, however you must:

- Write down the name, position and organisation of the person requesting the data
- Where it is practical to do so and the delay will not increase any risk of injury or death, seek the authorisation of a manager
- As soon as possible thereafter you must inform your manager and complete the “Data Disclosure Request” form, noting on the form that it is a retrospective submission on behalf of the member of the emergency services

7.7. Public Domain

Information that is already in the public domain is exempt from this policy

7.8. Subject Consent
In some cases, the college will request consent to process data, usually this is limited to marketing purposes. Students will be asked for consent at point of enrolment, and can withdraw consent at any time.

Any persons sending marketing or promotional materials on behalf of the college must ensure materials are only sent to persons who have consented to receive them.

7.9. Data Register
A data register will be maintained by the Data Protection Officer which documents processing activities undertaken by the college. This will detail the purpose of processing, the lawful basis for processing, and data retention period.

7.10. Lawful Basis
Data must only be processed where we have a lawful basis for doing so. UK GDPR defines six lawful basis for processing.

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interest

The lawful basis under which we carry out each data processing task we perform is documented in the data register.

7.11. Examination Marks

Students will be entitled to information about their marks for both coursework and examinations, however they may not be released prior to results publication dates.

The college may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned.

7.12. Retention of Data

A full list of information with retention times is available from the Data Protection Officer and detailed in the Archive policy.

7.11 Reporting of Breaches

The ICO defines a data breach as:

“A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to,

personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data."

Examples of breaches include, but are not limited to:

- Data corruption
- Computer Malware/Virus
- Hacking
- Unescorted visitors in secure areas
- Break-ins
- Thefts from buildings
- Thefts from vehicles
- Loss of data in transit (i.e. missing post)
- Insecure disposal of data
- Unauthorised disclosures
- Inappropriate sharing

Suspected data breaches must be reported immediately upon discovery to the Data Protection Officer, or if they are unavailable the COO or CEO.

The Data Protection Officer will instigate the data breach procedure to contain and investigate the breach.

Personal data breaches must be reported to the Information Commissioners Office (ICO) within 72 hours of their discovery. Breaches must only be reported to the ICO by the Data Protection Officer, or if they are unavailable the COO or CEO.

8. Related Policies

- Information Security Policy
- Acceptable use of ICT Policy
- Archive Policy
-
- Public Interest Disclosure Policy
- Safe Guarding Policy and Procedure
- Staff Disciplinary Procedure and Procedure