Data Protection (GDPR) Policy

Policy review area	All TEC (Trent Education Centre) Group. E.g. All Staff; Students; Governors; External partners; Visitors; Contractors and Sub-contractors; Member of the Public.
Lead manager	Principal
Approval level	Board
Start date	September 2019
Review cycle	2 year
Next review	August 2021

1. Executive Summary

TEC (Trent Education Centre) is required to keep and process personal information about staff, students, apprentices, contractors, visitors, governors and others. We recognise that having controls around the collection, use, retention and destruction of personal data is important in order to comply with our obligations under data protection laws and in particular our obligations under Article 5 of General Data Protection Regulation (GDPR) and processing activity requirements as set out in the Data Protection Act 2018.

This policy forms part of our **Information Governance Framework** which demonstrates how we as an organisation will comply with the core principles of the GDPR - see Appendix 1.

2. Responsibilities

This policy is in place to ensure that TEC (Trent Education Centre) is aware of its responsibilities under data protection laws. Protecting the confidentiality and integrity of personal data is a key responsibility of everyone within TEC (Trent Education Centre) and as such we are obliged to comply with this policy at all times to minimise the potential risk of damage and distress to Individuals (Data Subjects) and also the risk of penalties, fines, legal action and reputational damage to our organisation.

All those within TEC (Trent Education Centre) must comply with this policy and:

- Must ensure that they keep confidential all personal data that they collect, store, use and come into contact with during the performance of their duties.
- Must not release or disclose any personal data to anyone not authorised to access the personal data internally or outside TEC (Trent Education Centre) - this includes phone calls and emails.
- Must take all steps to ensure there is no unauthorised access to personal data whether by others within TEC (Trent Education Centre) who are not authorised to see such personal data or by people outside the organisation.

3. Data Protection Law Definition

The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of personal data and privacy and any applicable codes of practice issued by the Information Commissioners' Office (UK Regulator) including the UK Data Protection Act 2018 which makes provision above the processing of personal data and ePrivacy legislation.

This policy also has due regard to the Freedom of Information Act 2000 and associated legislation and guidance.

4. Accountability

The GDPR requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles". **This is the concept of Accountability.**

Accountability requires compliance with the GDPR to be documented. It is not enough to comply; we have to be able to demonstrate that we are complying through documentation. An overview of how we will comply with the GDPR is set out in the **Information Governance Framework** – Appendix 1.

5. Data Protection Principles

In accordance with the requirements outlined in the GDPR and DPA2018, personal data must be:

1. **Processed lawfully, fairly and in a transparent manner**
   We must be transparent with Individuals (Data Subjects) about how we will use their personal data. This is generally done through our Privacy Notices. The information that needs to be provided is set out in Article 13 and 14 of GDPR.

2. **Collected for a specified purpose, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes**
   Personal data must not be collected for one reason and then processed for another unless we have informed the individual. Our Privacy Notices will normally specify that some personal data may be used for a variety of purposes.

3. **Adequate, relevant and limited to what is necessary**
   Personal data collected must be necessary for the purposes for which it is being processed and not be collected "just in case" and forms that are used to collect data will be reviewed to determine whether any sections can be made optional.

4. **Accurate and kept up-to-date**
   Meaning that every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified as soon as possible and understanding the purpose for which personal data has been collected and is being used and ensuring that irrelevant personal data is not collected. This is known as data minimisation. Checks will be carried out on a regular basis to ensure that the data held is accurate. If the data is inaccurate or has changed, we will take steps to make sure that it is erased or rectified.

5. **Kept for no longer than is necessary for the purposes for which it is being processed** We should not keep personal data for longer than it is needed. This is not a "one size fits all" basis and when personal data is no longer needed, it should be securely deleted/destroyed in accordance with retention periods outlined in the Data Retention Policy. Some records relating to former students or employees may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

6. **Processed in a manner that ensures appropriate security of the personal data**
   It is a requirement of GDPR that appropriate technical and organisational security measures are used, monitored, controlled and audited to protect against unauthorised processing, accidental loss, destruction or damage of personal data. We take security very seriously and have in place policies, procedures and technologies to maintain the security of personal data.

6. Personal data and Special Categories of Data

The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria:

'Personal Data' (is clearly defined in Article 6 of the GDPR)	Any information relating to a 'living individual/identifiable person' (data subject) who can be directly or indirectly identified by reference to an identifier e.g. name, identification number, location data or online identifier. any information which relates directly to an individual and can be linked directly to them.
'Special categories of personal data' (are clearly defined in Article 9 of the GDPR)	The special categories are race, ethnic origin, politics, religion, trade union membership, health, sex life or sexual orientation and specifically include genetic data, and biometric data where processed to uniquely identify an individual. **Criminal Offence and Convictions -** Do not fall in the scope of Personal data, however, there are restrictions in processing defined in Article 10.
Anonymised Personal Data	Data which has been anonymised properly cannot be traced back to the original individuals in any way but can still be processed by organisations to conduct research. Fully anonymous data is not covered by GDPR as it contains no personal information to protect.
Pseudonymised Personal data	Data which has been properly pseudonymised can only be connected back to an individual using a specific 'key' or code. This can be an extra layer of security, but the data is still treated as Personal Data under GDPR because of the possibility of personal identification.

For the purpose of this policy, **personal data** refers to information that we collect and process, for example it relates to an identifiable, living individual for example a member of staff who could be identified directly or indirectly by gender, job role and office location if you can work out who they are. In our organisation, we will process **personal data** and in some cases **special categories of data** and **criminal conviction and offence** data for the following Individuals (Data Subjects), these are explained in more detail within our Privacy Notices:

- Employee (current and former)
- Student/Apprentice (current and former)
- Recruitment Candidate
- Parent/Legal Guardian/Carer/Next of Kin/Emergency Contact
- Volunteer
- Contractor/Sub-Contractor
- Consultant/Freelancer
- Board Member/Governor
- Work Experience Student or Intern
- Customers/Client/Service Users
- Training Delegate
- Visitors
- Member of the public

7. Data Controller, Data Processor and Joint Controller definitions

TEC (Trent Education Centre) is a **"Data Controller"** and a **"Data Processor"** of personal data and in some instances may also be a **'Joint Controller'**.

- A "**Data Controller**" is any entity (company, organisation or person) that determines the purpose and means of processing personal data e.g. makes its own decisions about how it is going to collect and use the personal data. A Data Controller is responsible for compliance with data protection laws. Examples of personal data we are the controller of are staff details or information we hold about students.
- A "**Data Processor"** is any entity (company, organisation or person) which accesses or processes personal data on behalf of the data controller e.g. When a third party, usually an outsourced service or a service provided by an external service provider involves access to or use of personal data, examples include software support for a system which contains personal data

which is provided by someone outside the organisation, cloud-based systems and mail fulfilment services.

- A **"Joint Controller"** is where two or more Data Controllers jointly determine the purpose and means of processing personal data e.g. joint activities. Two examples are:

1. The CCTV cameras are operated by 'Kadima Properties UK Ltd' and shared with other organisations such as 'Bridalwear'. They are involved in deciding how the CCTV System is run and what the images it captures are used for. They are both joint Data Controllers in relation to the personal data processed in operating the system.
2. Where both Data Controllers are involved in the decision-making process of how personal information will be collected and processed. It does this in partnership with local police and are responsible for the accuracy of the data it provides.

8. Information Commissioner's Office (ICO)

The ICO is the UK's data protection regulator (Lead Supervisory Authority).

TEC (Trent Education Centre) subsidiary companies are registered as "Data Controllers" with the Information Commissioner's Office as follows:

TEC (Trent Education Centre)	Registration No: Z3126380
LD Training Services LTD	Registration No: Z1881401
Vernon Community College CIC	Registration No: Z3100186

9. Accountability (Data Protection Officer)

As a publicly funded organisation we are required to have in post a Data Protection Officer (DPO). The Data Protection Officer will report directly to the CEO (Chief Executive Officer). The DPO's duties will include:

- Informing and advising TEC (Trent Education Centre) about their obligations to comply with the GDPR and other data protection laws by ensuring employees receive appropriate training and data protection awareness communications.
- Monitoring compliance with the GDPR and other data protection laws
- Managing internal data protection activities
- Advising on data protection impact assessments
- Conducting internal audits and investigations
- Providing GDPR compliance updates to the Corporation

10.Register of Processing

"Processing" is the collection, recording, organisation structuring, storage, adoption or alteration, retrieval, consultation or use, disclosure, destruction or erasure of personal data.

We will identify the legal basis for processing **'personal data'** as defined by Article 6 of the GDPR and **'special categories of data'** as defined by Article 9 of the GDPR and document this on Departmental Audits which together form our Register of Processing as required by Article 30 of the GDPR.

We need to assess which lawful purpose applies to make each use of personal data lawful. If the use changes then the assessment will need to be redone. The use of personal data will be reviewed periodically and any initial data audits will be updated periodically too. If we are considering making changes, we will decide whether their intended use requires amendments to be made and any other controls which need to apply and we may need to notify Individuals (Data Subjects) about the change.

11.Lawful Processing of Personal Data

We must ensure that the collection and use of personal data is lawful, this means that any use of **'personal data'** must fall within a "lawful purpose".

Lawful Basis	Examples
Contractual Obligation	The processing is necessary for a contract we have with an individual or third party or specific steps we are asked to take before entering into a contract **e.g. Terms and conditions of employment/Payroll Info/Adult Learner Agreements and supplying goods and services to organisations.**
Legal Obligation	The processing is necessary for us to comply with the law (not including contractual obligations). There are many lawful obligations which we must fulfil **e.g. Tax/Pension/Compliance with Health & Safety at Work Act/Equality & Diversity/providing education to under 18s etc**. We must process personal data lawfully if the data processing falls within this category, however, in most cases Public (Task) Interest will also apply.
Vital Interest	The processing is necessary to protect someone's life. Emergency information **e.g. in cases of life or death.**
Public Interest (Task)	The processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law. **We are a public body so can use Public Interest (Task) as a basis for processing, but if the processing is separate from the core college activities, then we must consider whether consent or legitimate interests are appropriate.**
Legitimate Interest	The processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the Individual's (Data Subject's) personal data which overrides those legitimate interests. This basis is also governed by rules on electronic communications (PECR/E Privacy Law – Privacy and Electronics Communications Regulations) so consent may be sought instead. **As a public body, we cannot rely on the lawful purpose of legitimate interests where the processing is in the performance of a task carried out in the public interest or in the exercise of official authority e.g. our core activities. Instead, we need to rely on the processing being necessary for the performance of a task carried out in the public interest. We may use it for areas such as marketing, fundraising or selling items such as tickets for events and equipment.**

Consent	The Individual (Data Subject) has given clear consent for us to process their personal data for one or more specific purposes **e.g. Photographs/videoing, academic results and achievement, biometric data using details for marketing activities.** Consent accepted under the DPA 1998 will be reviewed to ensure it meets the standards of the GDPR, however, acceptable consent obtained under the DPA will not be reobtained.

Consent must be:

- Freely given
- Specific
- Informed
- An unambiguous indication of an Individuals (Data Subjects) wishes
- A form of firm confirmation or positive opt-in, such as ticking boxes on a webpage
- Easily able to be withdrawn

Consent, cannot be obtained from the following:

- Silence
- Pre-ticked boxes
- Inactivity

Consent cannot be used in an employer and an employee relationship. The reasoning behind this is that the relationship is imbalanced and so the employee cannot really refuse to give their consent, for similar reasons, we may find consent difficult to rely on wherever there is a position of power e.g. over students.

Marketing and Consent

We may sometimes wish to contact Individuals to send them marketing or promotional materials, we will do this in a legally compliant manner by providing detail in their privacy notices, including for example whether profiling takes place and we will ensure that we obtain an individual's "clear affirmative action" giving un-ticked opt-in boxes. We will also consider other data privacy laws which sit alongside data protection in relation to direct and electronic marketing. We will follow ICO Marketing Guidance.

We will keep records documenting how and when consent was given, these may be held in a variety of storage mechanisms depending on the type of data and/or consent required. This information will be readily available for staff to check that consent has been obtained e.g. use of student photographs.

Withdrawal of Consent

"Consent" can be withdrawn by the individual at any time. It is therefore extremely important that due consideration is given to any processing activities whereby data is shared or processed and becomes outside the control of TEC (Trent Education Centre) for example printed materials, press releases etc. as we will be unable to exercise certain individual rights. In these instances, specific "informed" consent will need to be obtained.

12. Lawful purposes for processing 'Special Categories of Personal Data'

There are additional conditions which need to be met in order to use Special Categories of Personal Data. These are set out in Article 9 and are as follows (paraphrased):

- Explicit consent
- Employment and social security obligations
- Vital interests
- Necessary for establishment or defence of legal claims
- Substantial public interest
- Various scientific and medical issues.

13. Individuals' (Data Subjects) rights under the GDPR

Individuals' (Data Subjects) have certain rights under the GDPR; these rights are explained below together with details of how we will ensure these rights are met:

The right to be informed/Sharing Personal Data (Privacy Notices)
The GDPR requires us to inform Individuals (Data Subjects) of our personal data processing activities, we will do this through:

- Website Privacy Policies/Cookie Notices
- Student/Apprenticeship Privacy Notice
- Workforce (Staff) Privacy Notice
- Recruitment Candidate Privacy Notice
- Privacy Notice for "Other Individuals" e.g. non students and staff

Privacy Notices will be available on the TEC (Trent Education Centre) website. Paper versions are available on request.

The right of access

- Individuals (Data Subjects) have the right to obtain confirmation that their data is being processed and the right to submit a data subject access request (DSAR) to gain access to their personal data in order to verify the lawfulness of the processing or obtain copies of their records for other purposes. Data Subject Access Requests should be made via the Data Protection Officer – see 'Contact Section' below.
- Further information on how to make a DSAR request, together with information on Third Party Requests and Police/Enforcing Body Disclosure Requests are available on our website Data Protection page.
- TEC (Trent Education Centre) staff will follow the **Individual Rights Procedure** and **Data Subject Access Request Procedure -** See Flowchart at Appendix 2.
- We will maintain a Data Subject Access Request Register.

The right to rectification

Individuals (Data Subjects) are entitled to have inaccurate or incomplete personal data rectified on request via the relevant TEC (Trent Education Centre) Subsidiary Department. Upon receiving a request for rectification, we will:

- Check the validity of the request e.g. confirm identity of the person requesting the change.
- If the request is valid, amend the information where possible and record the actions taken.
- Where the personal data in question has been disclosed to third parties, we will inform them of the rectification where possible and where appropriate, we will inform the individual about the third parties that the data has been disclosed to.
- We will aim to deal with requests for rectification as soon as possible. We will respond within one month; this will be extended by two months where the request for rectification is complex
- TEC (Trent Education Centre) staff will follow the **Individual Rights Procedure -** See Flowchart at Appendix 5.
- Where we make a decision to take no action in response to a request for rectification, we will explain the reason for this to the individual and will inform them of their right to complain to the ICO.

The right to erasure (the right to be forgotten)

Individuals (Data Subjects) hold the right to request the erasure (deletion) or removal of personal data where there is no lawful basis for its continued processing, on request via the relevant TEC (Trent Education Centre), in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws their consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed.
- The personal data is required to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services e.g. selling goods or services on-line; to a child.
- In a marketing context, where personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the personal data must not be processed for such purposes.

We have the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes.

- The exercise or defence of legal claims.
- Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
- Where personal data has been made public within an online environment, we will inform other organisations who process the personal data to 'wherever' possible erase links to and copies of the personal data in question. We may not be able to exercise the right to erasure where content has been downloaded or re-shared.
- Where personal data has been used for printed materials such as marketing leaflets and prospectuses, we may no longer have control once published and therefore may not be able to exercise the right to erasure, where this is likely to apply we will state this in our request for consent.
- Where it is deemed that an adult or a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention must be given to existing situations where consent to processing has been given and they later request erasure of the data, regardless of age at the time of the request.
- **We will aim to deal with right to erasure requests within one month**, where we are unable to complete the request within this timescale, we will inform the individual.
- TEC (Trent Education Centre) staff will follow the **Individual Rights Procedure -** See Flowchart at Appendix 5.

The right to restrict processing

Individuals (Data Subjects) have the right to request us to block or suppress processing of their personal data.

Where a restriction may affect TEC (Trent Education Centre) carrying out their legal and contractual obligations or it is believed that the data is being processed under the Public Interest, Vital Interest or Legitimate Interest conditions of processing, we will follow guidance from the Information Commissioner's Officer to determine whether the request is valid and where possible temporarily stop processing until the validity of the request is determined.

If a request is determined to be valid, we will take steps to immediately restrict processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until we have verified the accuracy of the data.
- Where an individual has objected to the processing and we are considering whether our legitimate grounds override those of the individual.
- Where processing is unlawful and the individual opposes erasure and requests restriction instead.
- Where we no longer need the personal data, but the individual requires the data to establish, exercise or defend a legal claim.
- If the personal data in question has been disclosed to third parties, we will inform the third party about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

- Where processing is restricted, we will store the personal data, but not further process it guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
- We will inform Individuals (Data Subjects) when a restriction on processing has been lifted. TEC (Trent Education Centre) staff will follow the **Individual Rights Procedure -** See Flowchart at Appendix 5.

The right to data portability

Individuals (Data Subjects) have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller.
- Where the processing is based on the individual's consent or for the performance of a contract.
- When processing is carried out by automated means.

We are not required to adopt or maintain processing systems, which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual.

Personal data will be provided in a structured, commonly used and machine-readable form, free of charge, and where feasible, data will be transmitted directly to another organisation at the request of the individual. Requests should be made to the relevant TEC (Trent Education Centre). Upon receipt we will:

Respond with within one month or; Within one month advise the individual if we need to extend the timeframe by two months, where the request is complex, or a number of requests have been received:

- Where no action is being taken in response to a request, we will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the ICO.
- TEC (Trent Education Centre) staff will follow the **Individual Rights Procedure -** See Flowchart at Appendix 5.

The right to object

We will inform Individuals (Data Subjects) of their right to object at the first point of communication, and this information will be outlined in our Privacy Notices and explicitly brought to the attention of the individual (data subject), ensuring that it is presented clearly and separately from any other information. Where possible we will provide mechanisms for you to exercise your right to object, contact details within consent requests and Privacy Notices. We will aim to deal with requests within one month and advise you if we cannot meet this timescale.

Individuals (Data Subjects) have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest; Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- We will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims or where we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- We will stop processing personal data for direct marketing purposes as soon as an objection is received.
- We cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, we will offer a method for Individuals (Data Subjects) to object online.

14. Profiling and Automated decision making

Profiling and automated decision making are two different things although automated decision making can include profiling. We will specify any profiling or automated decision making in our Privacy Notices.

- **Profiling** happens where we automatically use personal data to evaluate certain things about an Individual e.g. any element of analysing or predicting behaviours or preferences (e.g. staff utilisation reports, analysis of performance at work). Profiling can therefore happen even if the ultimate decision is not taken by a machine and
- **Automated Decision Making** is where a decision is made about an Individual based solely on automated means without any human involvement and the decision has legal or other significant effects.

Individuals (Data Subjects) have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.
- We will take steps to ensure that Individuals (Data Subjects) are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, we will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.
- Automated decisions will not be applied to children or be based on the processing of Special Categories of data**, unless:**
  - The explicit consent of the child (or person with parental responsibility/legal guardian) is obtained.
  - The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

Members of staff will follow the **Individual Rights Procedure** and **Data Subject Access Request Procedure** to ensure compliance with data protection requirements – See Appendix 2 and 5 below.

15.Privacy by Design and Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is mandatory when processing is 'likely to result in a high risk' to the rights and freedoms of natural persons. Where we plan to adopt a new process, product or service which involves personal data, which is likely result in a high risk, we will act in accordance with data protection legislation. We will adopt a privacy by design approach and implement technical and organisational measures, which demonstrate how we build data protection into our processing activities reducing any risks to Individuals (Data Subjects) and potential reputational damage and fines or penalties.

Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive, please check the ICO website for full details):

- Large scale and systematic use of personal data for the purposes of Automated Decision Making or Profiling where legal or similarly significant decisions are made.
- Large scale use of Special Categories of personal data, or personal data relating to criminal convictions and offences e.g. the use of high volumes of health data.

- Systematic monitoring of public areas on a large scale e.g. CCTV cameras.
- To identify the most effective method of complying with our data protection obligations and meeting Individuals (Data Subjects)' expectations of privacy.
- To ensure all necessary parties are involved from the planning stage of a project e.g. implementation of new systems or a change to the way we process data.
- To assess appropriate safeguards are in place where personal data is intended to be transferred outside the EEA. Transfer includes sending personal data outside the EEA – see Transfer out the EEA section.
- To allow us to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to our reputation, which might otherwise occur.
- To assess whether new technologies or processing is likely to result in a high risk to the rights and freedoms of Individuals (Data Subjects) or;
- To enable the Data Protection Officer to consult the ICO to seek its opinion as to whether the processing operation complies with data protection legislation.

All DPIAs must be reviewed and approved by the Data Protection Officer.

All TEC (Trent Education Centre) staff will follow the **Data Protection Impact Assessment (DPIA) Procedure** – see flowchart **Appendix 3**. A central register of our Data Protection Impact Assessments will be maintained.

16.Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, for example 'deliberate, unauthorised and unintentional' incidents.

Whilst most Personal data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

There are three main types of Personal data breach which are as follows:

I. **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal data e.g. hacking, accessing internal systems to which you are not authorised to access, accessing personal data stored on a lost laptop, phone or other device, people "blagging" access to personal data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong member of staff or student, or disclosing information over the phone to the wrong person.

II. **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting personal data in error, loss of access to personal data stored on systems, inability to restore access to personal data from back up, or loss of an encryption key.

III. **Integrity breach** - where there is an unauthorised or accidental alteration of personal data.

Notifying breaches to the ICO

As an organisation we have to report breaches to the Information Commissioner's Office within 72 hours of detection where the breach is likely to result in a risk to the rights and freedoms of Individuals (Data Subjects). Failure to report a breach when required to do so may result in penalties and fines of up to €20 million, or 4% of an organisations global turnover.

Notifying breaches to Individuals (Data Subjects) affected

We will notify the Individuals (Data Subjects) affected by the Data Breach as soon as possible where the breach is likely to result in a high risk to their rights and freedoms, for example identity theft or fraud or where the breach may give rise to discrimination.

Whilst we are still required to notify the ICO, we are not obliged to notify the Individuals (Data Subjects) affected where:

- There are technological and organisational protection measures in place (e.g. encryption) We have taken action to eliminate the high risk.
- It would involve disproportionate effort – in this case Individuals (Data Subjects) must be informed some other way e.g. by a notice in newspapers.

Reporting a breach or concern

- Data breach and data concerns within TEC (Trent Education Centre) will be notified to the Head of Department and Data Protection Officer immediately as per the Data Breach Management Procedure - see flowchart at Appendix 4
- Data breach and data concerns from those outside TEC (Trent Education Centre) and within TEC should be made to the Data Protection Officer– see 'Contact Section' below.
- We will follow guidance from the ICO where necessary to determine if the breach is reportable.
- We will maintain a register of Data Breach incidents and concerns.

17.Transfer of Data outside the EEA

Data Protection Laws impose strict controls on personal data being transferred outside the EEA. Transfer includes sending personal data outside the EEA but also includes storage of personal data or access to it outside the EEA. It needs to be thought about whenever we appoint a supplier outside the EEA or we appoint a supplier with group companies outside the EEA which may give access to the personal data to staff outside the EEA.

Where it is necessary to transfer personal data outside the EEA, we will ensure that the organisation receiving the personal data has provided adequate safeguards in the Contract Variation or GDPR Compliance Agreement – see 'Third Party Processors/Joint Controller' Section. Individuals (Data Subjects)' rights must be enforceable and effective legal remedies for Individuals (Data Subjects) must be available following the transfer.

Personal data will not be transferred outside the EEA unless we have a signed GDPR Compliance Agreement confirming that adequate data protection legislation compliant safeguards are in place.

18.Third Party/Joint Controller Agreements

Data protection legislation requires us to ensure that we have a documented agreement with all our third party processors who have access to or process personal data on our behalf which confirms that they will comply with the requirements of data protection legislation and maintain adequate physical and IT security controls to protect our data, this will include ensuring appropriate safeguards are in place in relation to international personal data transfers and storage.

This means that if we plan to appoint any new third party 'Data Processors' of our personal data, we can only appoint them once we have carried out sufficient due diligence and we have a GDPR compliant contract or agreement in place.

We will also seek written confirmation from other authorised persons who are given access to personal data and systems that they will comply with TEC (Trent Education Centre)and TEC (Trent Education Centre)Group policies and procedures and that they will exercise appropriate physical and IT data security controls at all times.

We will obtain written agreements as follows:-

Processor Terms	**Our documentation**	**Their documentation**
Contract e.g. Contractors, suppliers, consultants, freelancers, system providers (Inc. cloud based systems)	Contract Variation document based on Standard clauses and/or wording as issued by Crown Commercial Services PPN 02/18 (May 2018), 'Changes to Data Protection Legislation & General Data Protection Regulation', amended for Colleges. See Appendix 5	Updated Contract/Terms and Conditions which matches those set out in our Contract Variation document.
Documented Agreements e.g. Funding Bodies and Partner Agency Agreements	GDPR Compliance Agreement	Signed GDPR/Compliance Agreement or Statement which matches the conditions set out in our GDPR Compliance Agreement or LA/Government Data Sharing Compliance Statement.
Validating/Awarding Body/Exam Boards	GDPR Compliance Agreement	Signed GDPR/Compliance Agreement or Statement which matches the conditions set out in our GDPR Compliance Agreement or LA/Government Data Sharing Compliance Statement.

Other Agreement (to include Freelancers/Consultants/Students and Apprentices/Stakeholders/Governors and other Individuals or companies whom we ask to process personal data on our behalf but do not fit into the categories above).	GDPR Compliance Agreement	Signed GDPR Compliance Agreement or Statement or Agreement which meet our GDPR requirements.
Joint Processors	GDPR Joint Controller Agreement as per Article 26 GDPR	Signed GDPR Compliance Agreement or Statement or Agreement which meet Article 26 GDPR requirements.

Future Monitoring of third party processors

We will monitor third party data protection compliance as set out in the GDPR Compliance Agreements or Contract terms, these may be by way of spot checks, reports and where necessary audits to ensure requirements in relation to Data Protection are being maintained.

19.Exemptions

Where applicable, we may apply exemptions available to us under the Data Protection Action 2018, Schedules 2, 3 and 4 which makes provision for exemptions from, and restrictions and adaptations of the application of, rules of the GDPR.

20.Data security

We will obtain and maintain Cyber Essentials Accreditation as a minimum standard to demonstrate our IT Security Management Systems are effective.

We will ensure that the physical security of our buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

TEC (Trent Education Centre), its employees and others with authorised access to personal data will ensure that appropriate IT and physical data security controls are used to protect unauthorised access to confidential records and personal data.

21.CCTV, videos and photography

We understand that recording images of identifiable Individuals (Data Subjects) constitutes as processing personal information, so it is done in line with data protection principles.

- **CCTV -** The CCTV Policy will be followed in relation to the use and purpose of CCTV monitoring across our various buildings and grounds. We will also set out the purposes for CCTV monitoring in our Privacy Notices.

- **Data Protection Impact Assessment –** We will carry out a Data Protection Impact Assessment in accordance with data protection legislation and guidance from the ICO and other official agency.
- **Photographs and non-CCTV recorded images** may be taken for a variety of purposes, these will be outlined on our Privacy Notices and we will normally make it clear as to the purpose at the time the photograph/video is being captured. Where we do not have a legal or contractual basis for taking photographs or recording/videoing of students, staff and others we will obtain consent from the individual concerned (or person with legal responsibility/legal guardian if under the age of consent or the person is deemed not capable of giving consent). Precautions will be taken, as outlined in the Learner IT Acceptable Use Policy in relation to the taking and publishing photographs of students, in print, video or on the TEC (Trent Education Centre) websites.
- **Images/videos captured by Individuals (Data Subjects) for recreational/personal purposes -** For clarification, images and videos captured by Individuals (Data Subjects) for recreational/personal purposes e.g. by a family member for family use are exempt from the data protection legislation, however, at times it may be necessary for us to ask you not to take photographs or use recording equipment for instance, events which may involve young children or vulnerable groups.

22.Concerns about your personal information

Concerns in relation to the processing of personal data, or the way your data privacy rights have been handled, can be directed to the Data Protection Officer in the first instance to enable us to investigate the concern(s). We will aim to carry out the internal review as soon as possible.

If you are dissatisfied with our response or if we fail to review your concerns, you have the right to escalate your concern directly to the Information Commissioner's Office (ICO). The ICO provides an online facility for reporting complaints which you will find at https://ico.org.uk/concerns/.

23.Related policies, procedures and guidelines

The following documents should be read in conjunction with this policy:

- *Data Retention Policy*
- *Data Protection Subject Access Request Procedure*

24.Contact

If you have any feedback about this policy or please contact the Data Protection Officer:

By Post: Data Protection Officer
TEC (Trent Education Centre)
292 Haydn Rd
Nottingham
NG5 1EB
United Kingdom

Email: dataprotectionoffice@trenteducation.co.uk

Telephone: +44 (0) 115 924 660

25. Appendix 1 Information Governance Framework