Independent Training
& Education Consultants

Data Protection and GDPR Policy

Last Reviewed: June 2021

By:

Directors: Susan Waters

Gerard Morrall

Signed by:  **Date: 30.06.21**

Contents

Policy Statement

Date of next review June 2022

ITEC is committed to a policy of protecting the rights and privacy of individuals, including learners, staff, and all others that we work with, in accordance with the Data Protection Act. ITEC needs to process certain information about learners, it is staff and stakeholders it has dealings with, for administrative purposes e.g., to pay staff, to administer courses and training, to record training progress, to book tests, and to comply with our legal obligations to funding bodies and government. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Organisation of Data Protection and Information

We will make sure that all personal data is:

- processed lawfully, fairly and in a transparent manner.
- collected for specified, explicit and legitimate purposes and is not further processed in a manner that is incompatible with those purposes.
- adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- accurate and, where necessary, kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- 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.

All our policies and procedures have been prepared in accordance with the General Data Protection Regulation (EU) 2016/679 (“GDPR”) and the Data Protection Act 2018.

Responsibility and Accountability.

- The Directors are responsible for developing and encouraging good information handling practice within the organisation.
- Gez Morrall is the nominated Data Protection Officer.
- Compliance with data protection legislation is the responsibility of all staff who have access to, and process information.
- Staff are responsible for ensuring that any personal data supplied to ITEC is accurate and up to date.

Principles of Data Protection and GDPR

Anyone processing personal data must comply with the eight enforceable principles of good practice. These state that data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant, and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to another country

Security Statement

ITEC has taken measures to guard against unauthorised or unlawful processing of personal data and against accidental loss, destruction, or damage.

- Adopting an information policy (this document is our policy)
- Taking steps to control physical security (learner and staff files are all kept in locked cabinets in an alarmed office)
- Putting in place controls on access to information (administrator for system, password protection, protected data files and limited data access)
- External partner providing professional IT support and security
- Training all staff on security systems and procedures
- Detecting and investigating breaches of security should they occur.

Learner Rights

Data protection law means that you have a range of rights over the personal data that ITEC collects and processes about you. There is a leaflet available called A guide to your rights – Personal Data, available from any ITEC member of staff.

- You have the right to know what data we have about you and what we are doing with it; this is known as the right to be informed.

Date of next review June 2022

- You have the right to make sure that the data we have about you is correct and complete; this is known as the right to rectification.
- In some circumstances you have the right to have your data deleted; this is known as the right to erasure, sometimes referred to as the 'right to be forgotten'.
- In some circumstances you have the right to ask us to stop processing your data; this is known as the right to restrict processing.
- For some of your data you have the right to ask us to provide you with an electronic version which you can then use elsewhere; this is known as the right to data portability.
- In some circumstances you can ask us to stop using your data; this is known as the right to object.

The law also gives you the right not to have decisions made automatically about you without a person being involved in the decision making: this is known as the right not to be subject to automated decision making, including profiling.

How can I make a request regarding my data?
The best way to make a request is to send an email to the data protection officer at gez.morrall@itec2016.com or you can use any of our normal channels of communication or talk to any member of staff.

In any circumstance you need to tell us:

- Your name and contact details
- Any information used by us to identify or distinguish you from other people with the same name, for example you Awarding Organisation registration number

Any details or relevant dates that will help us identify what data or action you want. For example, you may want to:

- Request a copy of your ILP or information file
- Ask us to delete an email address we are using to contact you with direct marketing
- Ask us to amend your contact details

How long will the process take?

We will usually deal with your request within o14 working days. If your request is complex we may extend the time we have to respond, but we would explain this to you within the standard 14 working days.

What if I am not satisfied?
If you are dissatisfied with how we have handled your request or you want to challenge a decision we have made you can raise your concerns with our Data Protection Officer at
gez.morrall@itec2016.com

If you are still dissatisfied you should can make a complaint to the ICO.
https://ico.org.uk/your-datamatters/raising-concerns/

ESFA Information:
The ESFA is responsible for funding education and skills in England for children, young people, and adults. It is also responsible for delivery of key services in the education and skills sector in England including the apprenticeship service, the provision of information, advice and guidance through the National Careers Service, and the Learning Records Service. We may use your personal information in our delivery of this work.

We collect your personal information where the law allows it, or we have a legal obligation to do so. Your personal information is collected to enable us to carry out the functions of the DfE.

The lawful basis for collecting and using your personal information will depend on the service and will normally be:

- where we need to for the purposes of Department for Education functions
- where we have your consent to do so
- where we have a legal obligation

If we are processing your personal information using your consent, you can withdraw your consent at any time.
Personal information is provided directly by you:

- face to face
- over the telephone
- via websites or subscribe to our mailings
- in emails

We may collect personal information about you from other systems or organisations funded by ESFA and from organisations that introduce you to us; so that we can contact you.

We may share your personal information with other services run by the ESFA, other parts of the DfE, and partner organisations, where the law allows it, or we have a legal obligation to do so:

Date of next review June 2022

- with a third party who is working for ESFA under contract
- with organisations for the purposes of:
    - administration
    - provision of career and other guidance
    - statistical and research purposes, relating to education, training, employment and well-being prevention or detection of crime.

Other organisations include:

- Department for Work and Pensions
- Local and Combined Authorities in England
- Greater London Authority
- Higher Education Statistics Agency
- Office for Standards in Education
- Institute for Apprenticeships
- educational institutions and organisations performing research and statistical work on behalf of the Department for Education, or partners of those organisations.

How long we will keep your personal information.

We will only keep your personal information for as long as we need it after which it will be securely destroyed.

We may need to keep your personal information indefinitely for research and statistical purposes. We will put in place necessary measures to safeguard this information.

Your data protection rights.

You have the right:

- to ask us for access to information about you that we hold
- to have your personal data rectified if it is inaccurate or incomplete.
- to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- to restrict our processing of your personal data (i.e., permitting its storage but no further processing)
- to object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you.

If we are processing your personal information using your consent, you can withdraw your consent at any time.

If you need to contact us regarding any of the above, please do so via DfE.

Contacting us about your information

If you would like:

Date of next review June 2022

- more information about how we process your personal information, or your data protection rights.
- to make a request about your information – for example to request a copy of your information or to ask for your information to be changed.
- to contact our Data Protection Officer

You can contact us by writing to:

Ministerial and Public Communications Division
Department for Education
Piccadilly Gate
Store Street
Manchester
M1 2WD

You also have the right to complain to the Information Commissioner's Office. Find out on their website how to report a concern.

Further guidance is available from the Information Commissioner's Office:

www.ico.org.uk

Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.

Personal information is collected by the ESFA in accordance with the terms and conditions of funding imposed on providers of learning, for example, further education colleges and private training organisations. Your personal information is processed by the DfE, and by those third-party organisations when they process your information on behalf of the DfE, to enable the DfE to carry out its functions. Learner information collected by the ESFA is known as the Individualised Learner Record (ILR). The specification and standards for the ILR are published for each

academic year (1 August to 31 July) by the ESFA. This specification provides more information about the use of your information.

Learner contact information collected by the ESFA may be used for the purposes of research and surveys to enable the DfE to carry out its functions or, where learning is funded by the European Social Fund (ESF), for the Department for Work and Pensions to carry out its functions. This contact information will only be used for the purposes of other research and surveys with the consent of the learner.
Learner information is also collected and supplied to the Learning Records Service, a part of the ESFA. Your information is used by the ESFA to issue learners with a Unique Learner Number, and to create and maintain your Personal Learning Record. More information about this use of learner information is published by the Learning Record Service.

Apprenticeships

As part of this service, individuals can apply for and be kept informed of apprenticeship opportunities. Your personal information is processed to match registered candidate requirements to vacancies for apprenticeships, including for those employers or providers offering a guaranteed interview scheme. Learning providers may act on behalf of employers to sift and shortlist candidates for interview that meet the criteria set by the employer. This service also enables the ESFA, and organisations funded to deliver the National Careers Service, and the Department for Works and Pensions (including Jobcentre Plus), and their employees or agents to search for apprenticeship vacancies and pass details to citizens and clients for the purpose of providing careers advice and guidance.
If you start an apprenticeship, your information is supplied to us by your employer to enable the DfE to carry out its functions. When you complete your apprenticeship, your information will also be shared with:

- an organisation appointed by your employer to assess the training that you receive.
- an organisation under contract to the DfE to issue you with an apprenticeship certificate.

This sharing is undertaken to enable the DfE and the Institute for Apprenticeships to carry out their functions.

LEARNER PRIVACY NOTICE

This privacy notice sets out the personal data ITEC collects about its learners and how that data is used and protected.

What data do we collect from you?
When you apply for a course

As part of your enrolment we will collect your personal details, this may include:

- your name, address, email address, telephone, date of birth, national insurance number, photograph, gender, ethnicity, disability, nationality, sexual orientation, religious belief, learning support needs, learning styles, employment status, LEA, benefits data, dietary requirements, where English is not first language, if you are a lone parent or asylum seeker, your refugee status, any offending background/previous convictions, health information, previous substance misuse, marital status, residency status, vehicle details for parking purposes, employment history, education history and qualifications, emergency contact details, voluntary work details, interests, references, where appropriate your carer details.

Whilst you are studying with ITEC

In order to manage and administer your education we will collect further data, this may include:

- course work, grades and results, exam entry details and results, attendance, tutor/personal tutor feedback, safeguarding information, accidents and injuries, first aid information, behavioural information, learner support needs, other support needs, placement data, withdrawal details, ICT usage.

- in order to manage the financial arrangements related to your study we may also collect and process your funding information, bank details, travel expenses details, your benefits and income data (or those of your household) and in some cases evidence.

- if you access additional learning support whilst you are studying we may collect and process further information including detailed health information, disabilities and support provided.

How we use your data

We will use your personal data;

- to manage and process your enrolment to ITEC
- to manage and administer your education whilst you are studying. This will include communicating with you, managing your timetable, putting together reports and registers, exam and assessment arrangements, personal tutoring, accessing ICT, accessing additional learning support and general learner support, safeguarding, health and safety, security, first aid, parking, managing behaviour, monitoring performance, handling complaints, ensuring equality;
- for the purposes of teaching you and measuring your achievements;
- to provide you with additional learning support;
- to maintain the health, safety and security of ITEC and all its users.

Marketing our courses to you

Where you have previously studied at ITEC or commenced an application process with us before, then we will send you information about the courses we provide on the basis of our legitimate business interests. In doing so, we will comply with the requirements of the 'soft opt in' and offer you an opportunity to refuse marketing, both when your details are first collected and in every subsequent message, by giving you a clear and straightforward way to unsubscribe.
Any other marketing we carry out will be on the basis of consent.

What is our legal basis for processing your data?
Generally, the data we collect about you is processed as part of our public interest task of providing education to you.

Where we collect health data this is defined as special category data we will process it because there is substantial public interest for us to do so.

Where we collect data to enable us to ensure and monitor equality of opportunity and treatment e.g. your ethnicity, disability, religious belief, sexual orientation this is defined as special category data. We process this data on the grounds that it is in the public interest, specifically by enabling us to identify and keep under review the existence or absence of equality of opportunity or treatment.
We also collect and process some personal data on the basis that we need to do so in order to comply with our legal obligations.

How we store and secure your data
Learner personal data is held electronically in password protected systems which are accessed by an authorised ITEC staff only. Hard copy student data is stored securely and accessed by authorised staff only.

Does anyone else process your data?
We do not use any third party data processors for our learner data.

Who do we share your data with?
We do not share information about our learners with anyone unless the law and our policies allow/require us to do so.

We may share your personal data with the following organisations (or types of organisation) for the following purposes:

- ESFA – if your course is funded by the ESFA we will share some of your data with the ESFA for the purposes of funding your education. Please see the ESFA section on page 5 for information about how they manage your data.

- Student Loans Company – if you have applied for a student loan we will share some of your data with the Student Loan Company in order to enable you to access your loan.

Date of next review June 2022

- Awarding bodies – if your course is accredited we will share some of your data with the relevant awarding body for the purpose of enabling you to gain your qualification.

- If you have a serious accident whilst at ITEC we may need to share that data with the Health and Safety Executive.

How long will we keep your data?
We will retain your personal data in line with the ESFA contract guidance and our retention schedule. Retention periods depend on the nature of the data being retained; in many cases we will retain your data for six years following the completion of your course.

DATA BREACH
Whilst ITEC takes information security very seriously, unfortunately it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of personal data. If this happens ITEC will investigate the breach.

Any staff who becomes aware of a potential breach of personal data is responsible for reporting it at the earliest possible opportunity to the Data Protection Officer.

A personal data breach is effectively any failure to keep personal data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of personal data. Whilst most personal data breaches happen as a result of action taken by a third party, they can also occur as a result of the actions of a member of ITEC staff.

There are three main types of personal data breach as follows:

Confidentiality breach – this is where there is an unauthorised or accidental disclosure of, or access to, personal data e.g. hacking, accessing internal systems that a staff member is 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 learner, or disclosing information over the phone to the wrong person.

Availability breach – this is 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. Lastly there is **Integrity breach** – this is where there is an unauthorised or accidental alteration of personal data,

An initial investigation into the potential breach will be undertaken by the Data Protection Officer immediately once notification is received.

This initial investigation will be used to inform whether an actual breach has occurred, and if so, what actions are required to contain it and what formal notification is required.

The Data Protection officer will assess the risks associated with the data involved, considering:

- its sensitivity
- the protections in place (e.g., encryptions)
- what has happened to the data e.g., has it been lost, corrupted, stolen?
- whether the data could be put to any illegal or inappropriate use
- who the individuals affected are, the number of individuals involved?
- the potential adverse effects on any data subjects (e.g., possibility of identity theft or other fraud/theft), how serious or substantial these are and how likely they are to occur.
- whether there are any wider consequences to the breach

Information from the ICO and the Article 29 Working Party guidelines on personal data breach notification will be used to inform this risk assessment process.

If it is established that the breach is unlikely to result in a risk to the rights and freedoms of the individuals affected, then it will be added to the data breach register and no further action will be taken.

Where it is established that a data breach has occurred which will impact on the rights and freedoms of the individuals affected then the Data Protection Officer will:

- Determine if the breach is still occurring, if so, steps will be taken to minimise the effects of the breach.
- Establish whether there is anything that could be done to recover any losses and limit any damage the breach could cause.
- Establish who needs to be notified as part of the initial containment and inform the police, where relevant or appropriate

Based on the outcome of the initial investigation and with due regard to data protection law and guidance provided by the Information Commissioner the Data Protection Officer, will determine who needs to be notified of the breach, they may

have to notify the ICO and possibly the individuals affected about the personal data breach.

The notification shall comply with the requirements of the ICO without undue delay and where feasible within 72 hours of when ITEC becomes aware of the breach unless it is unlikely to result in a risk to the rights and freedoms of individuals.

Notification to the ICO is mandatory where there is a likely risk to people. rights and freedoms because of a breach which could result in physical, material or non-material damage to natural persons such as:
• loss of control over their personal data
• limitation of their rights
• discrimination
• identity theft or fraud
• financial loss
• unauthorised reversal of pseudonymisation
• damage to reputation
• loss of confidentiality of personal data
• any other significant economic or social disadvantage to the person concerned

Breaches that are unlikely to result in a risk to the rights and freedoms of natural persons do not require notification to the ICO. An example might be. where personal data is already publicly available and a disclosure of such data does not constitute a likely risk to the individual.

If further investigation uncovers evidence that the security incident was in fact contained and no breach occurred the ICO will be notified. There is. no penalty for reporting an incident that ultimately transpires not to be a breach.

When reporting a breach, the following information will be provided:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned.
- the categories and approximate number of personal data records concerned.
- the name and contact details of the Data Protection Officer
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal. with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

RISK MANAGEMENT

ITEC has a risk management process to support business goals and to maintain compliance to legislation and awarding body requirements. We work with our governor to assess the risks to implementing new technology, systems, and information assets such as regulatory, financial, or operational risks. We have involved staff in information and training and promote embedding risk management across the organisation, this ethos is actively supported by the governor, the directors, and staff. In the event of any new procurement, the directors convene a meeting with the governor to discuss.

Before implementing any new system, equipment, or information process we consider any risk, identify advantages and disadvantages, and make decisions accordingly. We have taken the decision to contract the services of an external provider of IT Support to provide advice, guidance, and monitoring of IT systems to ensure compliance to regulatory bodies and legislation. Our provider of choice is Phase 5 Communications who are in our business village. Phase 5 have installed the relevant security systems, malware protection and network configuration to protect data and prevent data breaches. Phase 5 Communications monitor those systems monthly.

ITEC has achieved Cyber Essential Accreditation.

Staff induction includes an introduction to data protection and safe systems of work, with guidance provided by Phase 5 Communications. Staff have relevant permissions and access relative to their job role, the director responsible for GDPR has administration rights on the network system with a two-tier authentication on the account, he determines the level of access for staff in relation to their job role.
All staff have a photograph identification badge which enables access to the building, and which verifies identify.

Where relevant, staff complete online data protection updates or awareness each year and new staff complete the training as part of their induction, near the end of probation.

The Data Protection Officer handles all internal, restricted, or confidential information, and takes all reasonable steps to safeguard it. The Data Protection Officer ensures that he does not infringe copyright or break the terms of licences for software or other.
material. In all circumstances he does not attempt to access, delete, modify, or disclose Information Assets belonging to other people without their permission, unless it is obvious that they intend others to do this.

Portable storage devices are not permitted at ITEC, all learning resources are stored on the network system and the relevant permissions and access privileges have been put in place by the administrator. All administrative work is carried out in the

office, no data is worked on from home. In the event of prolonged home working a VPN solution has been recommended.

Transmission of personal information is minimal, and any email is encrypted for security.

Physical Security

ITEC is based in a secure business village with a manned reception, all offices are alarmed, and the building has entrances only accessed by key fob. Key fobs are only issued to staff working in the business village. The physical security of the site and the offices is the responsibility of the Business Village, Wilthorpe.

ITEC staff follow all physical security guidance provided by the Business Village and additionally operate a signing in register for learners and visitors. All staff wear a photo lanyard provided by the Business Village to identify them as ITEC staff.

In line with Covid-19 guidance the office is compliant to 2 metre ruling, there are hand sanitizers and additional signage for information.

Retention

Teaching and Learning		
Course Information	**Retention**	**Lead**
Records detailing information available about courses, programmes, departments, and facilities for learners.	Superseded +2 years	Directors
Policies & Procedures		
Records documenting the development and establishment of the institution's teaching procedures, strategy, and policies.	Superseded + 10 years	Director Teaching
Records documenting the development and establishment of the institution's teaching procedures.	Superseded + 5 years	Director Teaching
Records documenting the development of taught course assessment procedures.	Life of course	Director Teaching
Final versions of taught course assessment procedures.	Life of course	Director Teaching
Quality Assurance & Monitoring		
Records documenting the development of the institution's internal quality assurance processes.	While current	Quality Lead
Records documenting the conduct and results of formal internal reviews of teaching quality, and responses to the results.	Current year + 5 years	Quality Lead
Records documenting the conduct and results of external reviews and audits of teaching quality and standards.	Next Review completed + 5 years	Directors
Development & Execution of Courses		
Records documenting the process of obtaining approval and/or accreditation for taught programmes from professional, statutory, or other accreditation bodies.	Life of programme	Directors
Records containing data on, and analyses of, student numbers and other programme statistics.	Current year + 5 years	Directors
Records documenting routine solicited feedback on taught programmes from stakeholders	Current year + 3 years OR Life of course + 1 year	Directors
Records documenting the development of the institution's programmes, courses, and materials.	Life of course + 10 years	Directors
Working papers documenting the planning and conduct of teaching events.	Current year + 1 year	Director Teaching

Date of next review June 2022

Internal & External Review		
Records containing data on, and analyses of, student numbers and other taught course statistics. Records documenting routine solicited feedback on taught courses from staff and external examiners: individual feedback.	Current year + 5 years Current academic year + 3 years	Directors
Records documenting routine solicited feedback on taught courses from students: individual feedback.	Completion of analysis of feedback	Directors
Records containing reports of routine internal reviews of taught courses.	Current year + 5 years	Quality Lead
Records documenting the conduct and results of formal reviews of taught courses, and the responses to the results.	Current academic year + 5 years	Directors
Course Administration		
Timetabling of courses	Current year + 1 year	Director Teaching
Assignment of learners	Current year + 1 year	Director Teaching
Course assignment registers Learner and staff Learner data and personal information will be kept in line with the contract data. retention requirement. Apprenticeship data Staff data will be kept for the duration of employment plus 5 years.	Current year + 1 year ESF 31 December 2030 Current + 6 years Current + 5 years	Director Teaching Directors Directors

Date of next review June 2022

ICT Phase 5 Communication		
Records documenting the development and establishment of the institution's ICT systems strategy.	Superseded + 5 years	Phase 5
Records documenting the routine monitoring and testing of the operation of ICT systems, and action taken to rectify problems and optimise performance.	Current year + 1 year	Phase 5
Records documenting faults reported by users of ICT systems, and action taken to investigate and resolve the problem.	Last action on fault + 1 year	Phase 5
Records documenting the management of system data storage, including the operation of routine data backup, archiving and deletion routines.	Current year + 1 year	Phase 5
Records documenting the security arrangements for ICT systems.	Decommissioning of system + 5 years	Phase 5
Records documenting attempted or actual security breaches of the institution's ICT systems, and action taken.	Last action on incident + 1 year	Phase 5
Requests for, and authorisation of, connections of third-party equipment to the institution's networks, either on institutional premises or via dial-up communications links.	Termination of connection + 1 year	Phase 5
Records documenting the removal / return of mobile ICT systems hardware and software from / to the institution's premises.	Return of equipment + 3 months	Phase 5
Records documenting arrangements for the sanitisation of institutional ICT equipment prior to disposal.	Disposal of equipment + 1 year	Phase 5
Records documenting the development of technical and application training for ICT system users.	Superseded + 1 year	Phase 5

Secure storage of archived paper-based information has been purchased locally and the premises are secure and protected by alarm. Documents are stored in line with the retention schedule and ESF contract data retention requirements.

Destruction of archived paper-based information is undertaken in line with the retention schedule on site by a mobile shredding company.

Date of next review June 2022

Date of next review June 2022