Data Protection/GDPR and Security Policy

Date established:	May 2001
Updated:	Jan 2020
Reviewed:	Annually
Purpose:	This policy aims to set out MITSkills position regarding correct use of personal data according to the law

MITSkills is a learner centred private training provider working in the UK delivering training and skills valued by learners, employers, the community and the UK economy.

We regard the lawful and correct treatment of personal information held by MITSkills as very important to successful operations and for maintaining confidence between ourselves and those whom we deal with. We therefore make every effort to ensure that personal information is treated lawfully and correctly.

MITSkills needs to collect a range of personal information in order to operate. This includes information relating to current, past and prospective employees, suppliers, clients/customers and others with whom we communicate. MITSkills requires this information to support the administration of its operation and, in addition, it may occasionally be required by law to collect and use information of this kind to comply with the requirements of government departments for business data, for example. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this is in accordance with the Data Protection Act 2018.

We fully endorse and adhere to the principles of data protection, as detailed in the Data Protection Act 2018 and from 25 May 2018, the General Data Protection Regulation. The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union.

.

DATA PROTECTION/GDPR and SECURITY POLICY

1. INTRODUCTION

1.1 MITSkills is committed to protecting the rights and freedoms of data subjects, and safely and securely processing their data in accordance with all of our legal obligations.

1.2 We hold personal data about our employees, students, suppliers, contractors and other individuals/businesses for a variety of business purposes.

1.3 To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, MITSkills must comply with the Data Protection Act 2018 (the Act) and from 25 May 2018, the General Data

Protection Regulation. The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union.

1.4 This policy sets out how we seek to protect personal data and ensure that our stakeholders understand the rules governing their use of the personal data to which they have access in the course of their work or studies. In particular, this policy requires staff to ensure that MITSkills inline with GDPR the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

2. DEFINITIONS

Business purposes

The purposes for which personal data may be used by us:
Enrolment and funding, HR, administrative, financial, regulatory, payroll and business development purposes.
Business purposes include the following:
- Compliance with our legal, regulatory, funding and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering email and internet use for both staff and students)
- Operational reasons, such as enrolments of students, attendance marks on a register, images on CCTV, financial payments, exam marks, performance records, and protected characteristics.
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Marketing our activity – sharing student and staff success stories.

Personal data

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal data we gather may include: individuals' name, address, phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, protected characteristics. held, or going to be held on computer;
- in, or going to be in, a manual filing system that is highly structured so that information about you can be easily retrieved;
- in most health, educational, social service or housing records; or
- Other information held by a public authority.

Special categories of personal

Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition,

data	criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. SCOPE

3.1 This policy applies to all stakeholders, who must be familiar with this policy and comply with its terms.

3.2 This policy supplements our other policies relating to internet and email use for both staff and students and CCTV for which we have a separate policy which should be read in conjunction with this policy. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

3.3 Who is responsible for this policy?

MITSkills Limited as a corporate body is the data controller under the Act. However, the designated Data Protection Officer (DPO) will deal with day to day matters. *MITSkills designated Data Protection Officer is Hani Zubeidi, 01932 342416*

4. THE PRINCIPLES

4.1 MITSkills and all stakeholders shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles.

4.2 The Principles are:

1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we will be open and transparent as to how the data will be used.

2. Limited for its purpose

Data will only be collected for a specific purpose.

3. Data minimisation

Any data collected will be necessary and not excessive for its purpose.

4. Accurate

The data we hold will be accurate and kept up to date.

5. Retention

We will not store data longer than necessary.

6. Integrity and confidentiality

The data we hold will be kept safe and secure

4.3 Accountability and transparency

4.3.1 We will ensure accountability and transparency in all our use of personal data. We will show how we comply with each Principle. All applicable managers are responsible for keeping a written record of how all the data processing activities they are responsible for, comply with each of the Principles. This must be kept up to date and must be approved by the DPO.

4.3.2 To comply with data protection laws and the accountability and transparency Principle of GDPR, we will demonstrate compliance.

4.3.3 Managers are responsible for understanding their particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures.
- Maintain up to date and relevant documentation on all processing activities.
- Conducting Data Protection Impact Assessments.
- Implement measures to ensure privacy by design and default, including:
  - Data minimisation
  - Pseudonymisation
  - Transparency
  - Allowing individuals to monitor processing
  - Creating and improving security and enhanced privacy procedures on an ongoing basis

5. OUR PROCEDURES

5.1 Fair and lawful processing

5.1.1 We will process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

5.1.2 If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased. Consent to process individual's information will be taken at the point of application, and enrolment, for students, and at the point of signing a contractual agreement for staff and others.

5.2 Controlling vs. processing data

5.2.1 MITSkills Limited is classified as a corporate body and is the data controller under the act. We will maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully controlling and processing data.

5.3 Lawful basis for processing data

5.3.1 We will establish a lawful basis for processing data. Managers must ensure that any data they are responsible for managing has a written lawful basis approved by the DPO. It is the responsibility of each appropriate manager to check the lawful basis for any data they are working with and ensure all actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. Consent

We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. Contract

The processing is necessary to fulfil or prepare a contract for the individual.

3. Legal obligation

We have a legal obligation to process the data (excluding a contract).

4. Vital interests

Processing the data is necessary to protect a person's life or in a medical situation.

5. Public function

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. Legitimate interest

The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

6. SPECIAL CATEGORIES OF PERSONAL DATA

6.1 Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics

- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

6.2 In most cases where we process special categories of personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

6.3 The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

7. RESPONSIBILTIES

7.1 **All staff are responsible for:**

- checking that any information that they provide to MITSkills Limited in connection with their employment is accurate and up-to-date;
- informing MITSkills Limited of any changes to information, which they have provided. i.e. changes of address;
- checking the information that MITSkills Limited will send out from time to time, giving details of information kept and processed about staff;
- informing MITSkills Limited of any errors or changes. MITSkills Limited cannot be held responsible for any errors unless the staff member has informed MITSkills Limited of them;
- ensuring that personal data which they hold on students is kept securely (locked filing cabinet/drawer/on the network);
- not disclosing any personal data which they hold on students (orally, in writing or electronically) to an unauthorised third party without the prior consent of the Data Protection Officer or a Director
- ensuring that any data approved for disclosure and sent electronically must be encrypted and the encryption key sent separately;
- inform the Data Protection Officer of any proposed new uses of personal data

- comply with MITSkills's IT policy in relation to security;
- ensuring that 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 must comply with the above guidelines at Appendix one;
- destroying personal data according to MITSkills's Data Retention Policy.

7.2 **Students are responsible for:**

- checking that the information they provide to MITSkills in connection with their enrolment is accurate and up-to-date;

 informing MITSkills of any changes to the information they provide, such as, change of address, emergency contact details are notified using the "Correction of Personal Information On Student Record" form which is available from MITSkills Registry. This will enable MITSkills to update its Management Information System;
 ensuring that any personal data which they are required to provide as part of their enrolment is not disclosed (orally, in writing or electronically) to an unauthorised third party;
 not seeking to gain unauthorised access to personal information;
 complying with all MITSkills policies regarding the use of IT facilities.

7.3 **Managers are responsible for:**
 ensuring they are satisfied with the legality of holding and using the information collected by staff in their area;
 ensuring they keep MITSkills data documentation controller spreadsheet up to date based on their areas of responsibility;
 ensuring that the use of personal data complies with all appropriate MITSkills policies
 ensuring that relevant staff they manage, undertake the GDPR training;
 referring any non-routine requests for disclosure, requests for subject access and requests to cease processing to the Data Protection Officer;
 Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay;
 Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing.

7.4 **The Information Systems and Admin Team and DPO together are responsible for:**
Whilst all staff and users of personal data have some responsibility for the security of data, Information Systems staff (including Allware) and DPO together have an important role in ensuring the security of computerised data. In particular, they will:
 be responsible for advising MITSkills on the state of technological development with regard to IT security;
 provide secure methods of transferring authorised personal data outside MITSkills
 back up data on MITSkills's IT systems and have disaster recovery procedures in place and tested;
 implement virus detection and hacking preventative measures;
 through liaison with the appropriate manager, ensure that MITSkills's business systems are secure and appropriate restrictions

Individuals only have access to personal data in which they have a legitimate business interest;
 require the use of passwords and ensure they are changed regularly;
 produce and update policies for the use of MITSkills IT facilities including email, intranet and internet;
 investigate breaches of IT security;
 ensure that data is deleted according to MITSkills data retention policy.

7.5 **The Marketing Team are responsible for:**

- Approving data protection statements attached to emails and other marketing copy.
- Addressing data protection queries from clients, target audiences or media outlets.
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy.

7.6 **The Human Resources Manager will:**

- ensure that MITSkills Employment Practices are consistent with the Employment Codes of Practice
- ensure that Data Protection obligations are reflected in MITSkills Disciplinary Procedures and contracts of employment
- ensure that all staff are aware of the types of personal information that MITSkills will process on them and ask staff to check this information as required
- ensure that all obligations outlined within the Disclosure and Barring Service (DBS) Code of Practice published under section122 of the Police Act 1997 is adhered to. Full details of the CRB Code of Practice can be found at http://www.gov.uk/government/organisations/disclosure-and-barring-service
- provide advice to managers and others on the application of the DBS Code of Practice
- destroy personal data according to MITSkills data retention policy

7.7 **MITSkills Data Protection Officer will:**

- maintain MITSkills Data Protection registration;
- liaise with the Information Commissioner's Office and MITSkills legal advisers as required;
- make recommendations to MITSkills Leadership Team (MLT) regarding Data Protection/GDPR Policy and good practice;
- provide general guidance and advice and dissemination of information regarding Data Protection;
- Will ensure that where MITSkills use CCTV it is in line with the CCTV policy is adhered to and deal with all data requests related to CCTV in accordance with the policy and GDPR.
- Deal with subject access requests and co-ordinate responses;
- Co-ordinate and advice on all non-routine requests for disclosure of personal information;
- Monitor and report on data protection requests;
- Deal with any data breaches/complaints.

8. ACCURACY AND RELEVANCE

8.1 We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

8.2 Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

9. DATA SECURITY

9.1 Where other organisations process personal data as a service on our behalf, the GDPR working group on behalf of the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

9.2 Storing data securely:

- Data should be protected by strong passwords that are changed regularly and never shared between anyone else.
- Personal data should not be disclosed to unauthorised individuals, either within MITSkills or externally.
- Staff should ensure their account is locked at all times when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email unless the data is encrypted, as this form of communication is not secure.
- Data must be encrypted at all times before being transferred electronically.
- Staff should not save copies of personal data to their own computers, always access and update the central data.
- do not store data on removable media, such as USB and DVD drives.
- Data should never be saved directly onto Laptops or any other mobile devices such as Tablets or Smart phones.
- Staff should make sure paper and printouts with personal data are not left unattended where unauthorised access is available. All printouts to Photocopiers should be protected by an access code to release the print jobs.
- Printouts with personal data should be shredded and disposed of securely when no longer required.

10. DATA RETENTION

10.1 We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but will be determined in a manner consistent with our data retention guidelines. This is covered further in the Retention of Personal Data Policy.

11. TRANSFERRING DATA

11.1 As mentioned above, MITSkills collects a wide range of personal data relating to staff and students for its own purposes, and to meet external obligations. This may result in the eventual transfer of personal data to an outside third party, however any such transfers must be permitted under the Act. Personal data must not be disclosed to unauthorised third parties including another individual or organisation, family members, friends, local authorities, government bodies, and the police where the individual has not consented to the transfer unless disclosure is exempted by the Act, or by other legislation. There is no general legal requirement to disclose information to the police.

11.2 However data can sometimes be disclosed without consent, where, for example, it is required for:

 protecting the vital interests of the data subject (i.e. release of medical data in emergency)
 the prevention or detection of crime, fraud, or to ensure examination integrity for **CCTV images see MITSkills CCTV policy**

11.3 Transferring information to a third party (with the data subject's consent)
11.3.1 Personal Data can be transferred to another third party if the data subject has given their consent. This must always be in writing. Consent cannot be inferred from silence, so if the MITSkills requests consent so that personal data can be provided to a third party, and no response is received, the MITSkills must infer that consent is withheld.

11.3.2 Data may be shared for example with an external payroll company or the HMRC in regard to staff and with the relevant funding agencies, internal and external verifiers and internal and external auditors (please note that this list is not exhaustive).
11.4 Disclosure of information to a sponsor or prospective employers:
11.4.1 Often a third party, or prospective employer, may contact MITSkills to verify details about a student, such as attendance records and examination results. In most circumstances, students would not object to the disclosure of such information, and indeed it may benefit the student. However, the request for information should be accompanied by a statement from the student consenting to the disclosure, or the student should be contacted to confirm their consent.
11.5 Providing information because it is required by law:
11.5.1 MITSkills will disclose information in accordance with any legislation which it is subject to.
11.6 Transferring data securely
11.6.1 Every effort should be made to ensure that any data being transferred, regardless of whether electronic or otherwise, remains secure. Once authorisation has been given to transfer data externally, then Computer Services will provide the most appropriate secure method of transfer. (In some cases, the external organisation will stipulate that the data is transferred using their systems and therefore specific instructions will be provided). The originating member of staff should confirm safe receipt of the information from the recipient and highlight any potential losses to the Data Protection Officer immediately.

12. RIGHTS OF INDIVIDUALS

12.1 Individuals have rights to their data which we will respect and comply with to the best of our ability. We will ensure individuals can exercise their rights in the following ways:

Right to be informed
 providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.

• Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.
Right of access
 Enabling individuals to access their personal data and supplementary information
 Allowing individuals to be aware of and verify the lawfulness of the processing activities.

Right to rectification

 We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.

 This must be done without delay and no later than one month. This can be extended to two months with permission from the DPO.

Right to erasure

 We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

Right to restrict processing

 We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.

 We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

Right to data portability

 We must provide individuals with their data so that they can reuse it for their own purposes or across different services.

 We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

Right to object

 We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.

 We must respect the right of an individual to object to direct marketing, including profiling.

 We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

Rights in relation to automated decision making and profiling

 We must respect the rights of individuals in relation to automated decision making and profiling.

 Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

13. MAKING AN ENQUIRY

13.1 To obtain a copy of information held about you, to which the Data Protection Act/GDPR applies, you must detail in writing your request to MITSkills Data Controller. MITSkills will comply with the request within the statutory timescale unless there is good reason for the delay. In such cases, the reason will be explained in writing to the person making the request. You will be informed of the cost of your request following your submission, if the request is deemed free of charge please note a "reasonable fee" can be charged for further copies of the same information and when a request is manifestly unfounded or excessive, particularly if it is repetitive. The fee will be based on the administrative cost of providing the information.

Where your request is related to Data in the format of CCTV images the request must be made using the form provided **in MITSkills CCTV policy** – this is due the nature of such data a copy of the CCTV policy is available on our website or a copy can be obtained via contacting our Data Protection Officer

All enquiries about access to information should be addressed to the designated Data Controller/Data Protection Officer
Hani Zubeidi
Company Secretary and Data Controller
MITSkills Limited
10 Camphill Industrial Estate
West Byfleet
Surrey
KT14 6EW
:

14. DATA PORTABILITY REQUESTS

14.1 We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay and no later than one month. This can be extended to two months for complex or numerous requests, but you will be informed of the extension within one month.

15. RIGHT TO ERASURE

15.1 What is the right to erasure?
Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child (aged under 13)

15.2 Retention of Data and how we deal with the right to erasure:
We will consider each request for erasure on a case by case basis; we will only refuse to comply with a right to erasure in the following circumstances:

- 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, including compliance with funding regulations
- The exercise or defence of legal claims

All rights for erasure should be submitted to the DPO for consideration. Requests from individuals who have accessed government funding will be referred to MITSkills

retention of personal data policy for information in relation to data retention required by government bodies as follows

Retention of Data

i. MITSkills will keep some forms of information for longer than others, Information about learners cannot be kept indefinitely, unless there are specific requests to do so, In general information about learners will be kept for a period of ten years or 31st December 2030 (whichever is the latter) after they leave MITSkills as currently required to evidence access to funding which is a requirement of the ESFA and Department of Education as appropriate Data required to evidence funding can be erased after this date, and cannot be erased prior to this timescale unless the data subject has obtained written approval and evidenced this to MITSkills from the appropriate funding body. This will require MITSkills confirms such approval prior to agreeing erasure.

   This will include:

   - name and address,
   - academic achievements, including marks for coursework and
   - Copies of any reference written.

ii. All other information, including any information about health, race or disciplinary matters will be destroyed after 10 years of the course ending and the student or MITSkills.

MITSkills will need to keep information about staff for longer periods of time; In general, all information will be kept for five years after a member of staff leaves MITSkills. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. A full list of information with retention times is available from the data controller

16. THE RIGHT TO OBJECT

16.1 Individuals have the right to object to their data being used on grounds relating to their particular situation. We will cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise, and defence of legal claims or funding regulations.
- We will always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. Any objections should be submitted to the DPO.

16.2 The right to restrict automated profiling or decision making:
We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.

- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we will:
- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

All rights to object should be submitted to the DPO for consideration.

17. THIRD PARTIES

17.1 Using third party controllers and processors
17.1.1 As a data controller we will have written contracts in place with any third-party data controllers and/or data processors that we use. The contracts will contain specific clauses which set out our and their liabilities, obligations and responsibilities.
17.1.2 As a data controller, we will only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.
17.1.3 As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.
17.1.4 MITSkills maintains a full list of third-party companies (subcontractors); it is the responsibility of each relevant manager to ensure this document is kept up to date and is relevant.

17.2 Contracts
17.2.1 Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data controllers (and/or) data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.
17.2.2 At a minimum, our contracts must include terms that specify:
- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Retained as per MITSkills retention of personal data policy.
- Submit to regular audits and inspections and provide whatever information necessary for the controller and processor to meet their legal obligations.

- Nothing will be done by either the controller or processor to infringe on GDPR.

18. AUDITS, MONITORING AND TRAINING

18.1 Data audits

18.1.1 Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. This is in conjunction with the official MITSkills auditors.

18.2 Monitoring

18.2.1 All stakeholders must observe this policy. The DPO has overall responsibility for this policy. MIT Skills will keep this policy under review and amend or change it as required. You must notify the DPO of any breaches of this policy. You must comply with this policy fully and at all times.

18.3 Training

18.3.1 All staff will receive adequate training on provisions of data protection law specific for their role. All staff must complete all training as requested. If staff move role or responsibilities, they are responsible for requesting new data protection training relevant to their new role or responsibilities.

18.3.2 If staff require additional training on data protection matters, they must contact the Company Secretary (DPO).

19. REPORTING BREACHES

19.1 Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. MITSkills has a legal obligation to report any data breaches to the relevant supervisory authority within 72 hours.

19.2 All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the supervisory authority of any compliance failures that are material either in their own right or as part of a pattern of failures

19.3 Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

19.4 Please refer to the DPO for our reporting procedure.

20. FAILURE TO COMPLY

20.1 We take compliance with this policy very seriously. Failure to comply puts both staff and students, and MITSkills at risk.

20.2 The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

20.3 If staff or students have any questions or concerns about anything in this policy, they should contact the DPO.

21. RELATED POLICIES AND PROCEDURES

21.1 MITSkills has a number of policies/procedures which are associated with the Data Protection Policy policies include:

Use of Email and Internet Policy
Staff Management Policy
CCTV Policy

22. EQUALITY IMPACT ASSESSMENT

22.1 MITSkills is committed to the promotion of equality, diversity and providing a supportive environment for all members of our community. Our commitment means that this policy has been reviewed to ensure that it does not discriminate (either intentionally or unintentionally) any of the protected characteristics of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation and meets our obligations under the Equality Act 2010. Therefore, this policy has no adverse impact on any of the above protected groups.

Data Protection Appendix

Staff Guidelines for Data Protection

1. All staff will process data about students on a regular basis, when marking registers, or MITSkills work, writing reports, assessing caring out review, or using contact details or providing references, or as part of a pastoral or academic supervisory role. MITSkills will ensure through its enrolment procedures that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the Data Protection Act 2018 Act and (GDPR) (EU) 2016/679. The information that staff deal with on a day to day basis will be 'standard' and will cover categories such as:

- General personal details such as name and address
- details about class attendance, coursework marks and grades and associated comments
- notes of personal supervision, including matters about behaviour and discipline.

2. Information about a student's physical or mental health; sexual activities; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student's consent. Consent is obtained on the processing of ethnicity, faith and learning difficulty and/or disability data at enrolment. However, if staff need to record any other information, they should seek the student's written consent, for example, recording information about dietary needs, or health

reasons prior to taking students on a trip or visit; recording information that a student is pregnant.

3. Should a member of teaching staff consider it necessary to collect sensitive data or be asked to process this data, they should refer to the Company Secretary or Managing Director in the first instance.

4. The only exception to this will be if the staff member is satisfied that the processing of the data is necessary and:

 In the best interests of the student or staff member, or a third person or MITSkills

 He or she has either informed the authorised person of this or has been unable to do so and processing is urgent and necessary in all the circumstances.

This should only happen in very limited circumstances. E.g. a student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student is pregnant.
5. The relevant Company Secretary will be the DPO and will be responsible for ensuring that all data is kept securely.

6. Staff must not disclose personal data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the Data Protection Officer, or in line with MITSkills policy.

7. Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the data protection officer, or in line with MITSkills policy.

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

Deciding which data protection condition to rely on
If MITSkills are making an assessment of the lawful basis, we will first establish that the processing is necessary. This means the processing will be a targeted, appropriate way of achieving the stated purpose. We will not rely on a lawful basis if we can reasonably achieve the same purpose by some other means. Remember that more than one basis may apply, and staff should rely on what will best fit the purpose, not what is easiest.

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.
We must also ensure that individuals whose data is being processed by MITSkills are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.
If staff are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the DPO.
Staff Checklist for Recording Data
 Do you really need to record the information?
 What is the purpose for processing the data?

- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data

Date Reviewed	06/01/20
Reviewed	Annually
Version Status	Approved
Approved By:	 Company Director: Date 06/01/20