Quality Procedures and Policies	CEN-009	Issue Number	9
		Issue Date	March 2023
Data Protection and UKGDPR Compliance		Originator	PH
		Amended by	PH
		Approved by	PH

Ref.	Contents
1	**Introduction**
2	**Scope**
3	**Risk Management**
4	**Staff Identification**
4.1	Data Protection Officer
4.2	Data Protection Officer Support
4.3	Data Processors
4.4	Data Controllers
5	**Data Collection, Usage, Sharing and Erasure**
5.1	Apprentice Applicants
5.2	Apprentices
5.3	Learners on Commercial Courses
5.3.1	Regulated Qualifications
5.3.2	Unregulated Qualifications and Bespoke Courses
5.4	Staff
5.5	Employers
5.6	Subcontractors
6	**Procedures**
6.1	Data Subject Erasure Request and Procedure
6.2	Staff Training
6.3	Data Subject Access Request Procedure
6.4	Privacy Notice and Procedure
6.5	Retention of Records Procedure
6.6	Data Subject Consent Procedure
6.7	Data Subject Change Request Procedure

6.8	Complaints Procedure
6.9	Data Breaches
6.9.1	Breach Notification and Investigation Procedure
6.10	Information Security
6.10.1	Secure Disposal of Storage Media
6.10.2	Wireless Computer Security Procedure
6.10.3	Physical Entrance, Controls and Security Areas
6.10.4	Document Control Procedure
6.10.5	Electronic User Access Management
6.10.6	Electronic and Paper-based Records Access Control, Rules and Rights Policy and Procedure
6.10.7	Data Erasure Model
6.10.8	Laptop's Used Externally Off-Site
6.11	Internal Audit Procedure
6.12	Supply of Documents and Encryption
6.13	Data Portability Procedure
6.13.1	Apprentices and Their Employers
6.13.2	SETA employees
6.13.3	Commercial learners
6.14	Data Protection Impact Assessment Procedure (DPIA)
6.14.1	Data Protection Impact Assessment Register
6.15	Schedule of Authorities, Key Suppliers and Customers
6.15.1	Employers using SETA to Train their Apprentices and Learners
6.15.2	Privately Paying learners using SETA to Train Themselves
6.15.3	Suppliers
6.16	Clear Desk Policy
6.17	International Data
6.18	Server Backup
6.19	Network Protection
7	**Review**
8	**Contact**

1. Introduction

SETA will collect and retain certain information about its employees, learners, member companies and trustees. For example, to allow it to monitor staff performance, learner achievements and capture health and safety Data. It is also necessary to process information so staff can be recruited and paid, learners registered and certified on regulated qualifications, and legal obligations to funding bodies and government complied with. 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, SETA complies with the Data Protection Act 2018, which includes the General Data Protection Regulations (UK GDPR); this document sets SETA's framework for compliance.

2. Scope

SETA conducts business in the Training and Education sector across two sites; an apprenticeships Centre located in First Avenue and a Skills Centre located in Second Avenue. Data is collected within both centres and share a common computer Server. Therefore, many sources and types of information is collected from the following Data subjects:

- *Apprentice applicants*
- *Apprentices*
- *Learners on commercial courses*
- *Employers*
- *Subcontractors*
- *Staff*

Both 'Personal Information' and 'Special Categories of Personal Data' is obtained from these Data subjects during various stages of business, and SETA will ensure that all Data will be collected, processed and maintained in accordance with the registration under the Data Protection Act 2018.

SETA ensures it will only collect Data required and process it for the purpose it is intended for; SETA will not share any Data with any external organisation other than specified in section 4 of this document.

This document sets out how this is achieved and works in line with SETA's Privacy Policy **(Please see CEN-029 - Privacy Policy)**.

SETA has adopted the 'Privacy by Design' model and only collects Data that is required.

3. Risk Management

Key Risk Areas

SETA has identified risks within the organisation in two key areas:

1. Data being accessed by unauthorised people through poor security (**Annex A** gives details on this risk)
2. Individuals being harmed through Data being inaccurate or insufficient
   If an apprentice or learner is on SETA's PICSWEB Learner Management System (LMS) and registered on a regulated programme of study through an Awarding Body or Awarding Organisation and Data is not accurate, there is a risk that:
   a) *The learner's Certificate may be incorrect*
   b) *An apprenticeship completion might not be possible due to conflicting information*

   SETA has a robust Registration, Claims and Transfer process **(Please see COM-008 - Vocational Qualification Registration, Claims and Portfolio Control** and **COM-004 - Pearson Qualification Registration, Claims and Portfolio Control)**. The appropriate Centre Co-ordinator will contact the Awarding Body and/or Awarding Organisation when an error arises for risks 'a' and 'b' as above to correct or appeal it. Both risks identified in 'a' and 'b' above are 'Low Risks' due to the history and experience that SETA has had with similar issues having been corrected with ease.

4. Staff Identification

4.1 Data Protection Officer

SETA's Centre Compliance Manager acts as the Data Protection Officer, whose role is as follows (non-exhaustive):

- *to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State Data protection provisions*
- *to monitor compliance with this Regulation, with other Union or Member State Data protection provisions and with the policies of the controller or processor in relation to the protection of personal Data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits*
- *to provide advice where requested as regards the Data protection impact assessment and monitor its performance pursuant to Article 35 of the General Data Protection Regulation 2018*
- *to cooperate with the supervisory authority*
- *to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 of the General Data Protection Regulation 2018, and to consult, where appropriate, with regard to any other matter*
- *to meet regularly with the Chief Executive Officer and Chief Operating Officer to discuss issues, concerns and Data breaches*
- *to report Data breaches to the 'Information Commissioner's Office' (ICO)*

The Data Protection Officer shall in the performance of their tasks have due regard to the risk associated with processing operations taking into account the nature, scope, context and purposes of processing.

4.2 Data Protection Officer Support

The Chief Executive Officer and Chief Operating Officer will meet regularly with the Data Protection Officer to discuss issues, concerns and Data breaches. They will also support/assist the Data Protection Officer when a breach occurs.

4.3 Data Processors

The ICO defines a Data Processor as '*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*'.

The ICO defines 'Processing' in relation to information or Data as '*taking any action with someone's personal data. This begins when a data controller starts making a record of information about someone, and continues until you no longer need the information and it's been securely destroyed. If you hold information on someone, it counts as processing even if you don't do anything else with it'*.

SETA has adopted this ICO guidance in general, and Data Processors have been identified in **Annex C**

Within agreement with a Data Controller, SETA's Data Processors may decide:

- *what IT systems or other methods to use to collect personal Data*
- *how to store the personal Data*
- *the detail of the security surrounding the personal Data*
- *the means used to transfer the personal Data from one organisation to another*
- *the means used to retrieve personal Data about certain individuals*
- *the method for ensuring a retention schedule is adhered to*
- *the means used to delete or dispose of the Data*

4.4 Data Controllers

The ICO defines a Data Controller as '*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*'.

SETA, as a company is a Data Controller and has identified certain staff as 'Information Asset Owners' (IAO's), who are responsible for the various information assets they control. SETA's IAO's have been identified in **Annex D**.

The controller will:

- *ascertain the reason why personal Data is collected in the first place and the legal basis for doing so*
- *which items of personal Data to collect, (for example, the content of the Data)*
- *the purpose or purposes the Data are to be used for*
- *which individuals to collect Data about*
- *whether to disclose the Data, and if so, who to*
- *whether Data subject access and other individuals' rights apply (for example, the application of exemptions)*
- *how long to retain the Data or whether to make non-routine amendments to the Data*

5. Data Collection, Usage, Sharing and Erasure

Personal data is defined in the UKGDPR as '*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'.*

The ICO defines 'Special categories of personal data' as Data consisting of information as to:

a) *the racial or ethnic origin of the Data subject*
b) *their political opinions*
c) *their religious beliefs or other beliefs of a similar nature*
d) *whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)*
e) *their physical or mental health or condition*
f) *their sexual life,*
g) *the commission or alleged commission by them of any offence, or*
h) *any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings*

SETA recognises and uses these definitions as guidance.

5.1 Apprentice Applicants

SETA will collect only required Data on the Applicant when they have completed and returned Part A of the 'SETA Application for Training' form, which also includes a 'learner Data Subject Consent form' and a copy of SETA's Privacy Policy **(Please see CEN-029 - Privacy Policy)**. This Data will be collected by the Apprenticeship Services Manager and entered in to the PICSWEB LMS and uploaded to SETA's secured 'apprenticeship' server and deleted after a period of 1 year. SETA recommends that Applicants complete this form electronically and return it via e-mail to the Apprenticeship Services Manager via password encryption. If an Applicant returns a hand written form, it will be scanned in and the original destroyed by the Apprenticeship Services Manager by following '**6.10.7 - Data Erasure Model**'.

5.2 Apprentices

All documents in use by SETA staff as specified in '**6.10.6 Electronic and Paper-based Records Access Control, Rules and Rights Policy and Procedure**' and '**6.10.5 Electronic User Access Management**', contain both 'Personal' and 'Personal Sensitive' Data. All completed paperwork and documents are scanned and held electronically on SETA's secured Server for a period of 3 years after they have completed. The Apprenticeship Services Manager will destroy all completed paperwork and documents once they have been processed electronically by following '**6.10.7 - Data Erasure Model**'.

Only Data required will be shared electronically with the following Awarding Bodies and Organisations in line with their own Data sharing protocols and procedures for Qualification Registration and Certification purposes:

- *ECITB*
- *EAL/Enginuity*
- *City & Guilds*
- *Pearson*
- *TWI*
- *ImechE*
- *SIAS*
- *NOCN*

5.3 Learners on Commercial Courses

5.3.1 Regulated Qualifications

SETA delivers the following commercial courses regulated by the following Awarding bodies and organisations:

- *NET AAC, AM2 and AM2S*
- *EAL/Enginuity Level 2, Level 3 and /Level 4 NVQ's*
- *ECITB CCNSG Safety Passport, Refresher and LATS*
- *City & Guilds Electric Vehicle Charging (2921)*
- *City & Guilds Requirements for Electrical Installations (2382)*
- *City & Guilds Electrical Equipment Maintenance and Testing (2377)*
- *City & Guilds Initial and Periodic Electrical Inspection and Testing (2391)*
- *City & Guilds Design, Erection and Verification (2396)*
- *CompEx (JTL)*

SETA collects Personal Data either via SETA's own Application forms or those generated by the Awarding Bodies and Organisations for Registration and Certification purposes. All forms contain a 'learner Data Subject Consent form', a copy of SETA's Privacy Policy and SETA's 'Terms and Conditions' **(Please see CEN-029 - Privacy Policy)**. This Data will be shared electronically with the Awarding Bodies and Organisations in line with their own Data sharing protocols for Qualification Registration and Certification purposes only. All completed paperwork and documents are held in paper-based format in SETA's premises located in 1st Avenue in locked and secured filing cabinets for a period of 3 years. The Administration staff will destroy all completed paperwork and documents once they have been passed this time by following '**6.10.7 - Data Erasure Model**'.

5.3.2 Unregulated Qualifications and Bespoke Courses

SETA delivers the following commercial courses which are unregulated by any Awarding bodies and organisations:

- *Abrasive Wheels*
- *AM2 Examination Preparation*
- *Basic Electrical Appreciation*
- *Bespoke Electrical*
- *CAD*
- *Cross Skilling*
- *Bespoke Exxon Courses*

- *Mechanical Joint Integrity*
- *Machining*
- *Pipefitting*
- *Welding*

SETA requires Data to be collected via SETA's own Application forms for enrollment, which contains a 'Learner Data Subject Consent form', a copy of SETA's Privacy Policy and SETA's 'Terms and Conditions' **(Please see CEN-029 - Privacy Policy)**. SETA ensures it will not share this Data with any external organisation.

All 'Joining Instructions' are written letters that are either posted or e-mailed electronically to candidates with details of their course times, dates and instructor names. These letters are stored on SETA's secured server electronically, and are saved only in template format and will not contain any personal details.

All completed paperwork and documents are held in paper-based format in SETA's premises located in 1st Avenue in locked and secured filing cabinets for a period of 3 years. The Administration staff will destroy all completed paperwork and documents once they have been passed this time by following '**6.10.7 - Data Erasure Model**'

5.4 Staff

All staff employed at SETA will have their personal details, including special categories of personal data collected and held as part of HR requirements.

The following documents and Data are held at SETA in a locked filing cabinet which is only accessible by the Chief Executive Officer and Chief Operating Officer:

- *Application form for Employment*
- *CV*
- *Certificates*
- *DBS check results form*
- *Passport copy*
- *Driver's License*
- *Bank authorisation form*
- *Appraisals*

The Centre Compliance Manager also keeps the following documents for all staff for training and CPD purposes:

1. *CV*
2. *List of Qualifications*
3. *Certificates*
4. *DBS records*
5. *CPD Record*
6. *Assessment Documents*
7. *Internal Quality Assurance Documents*

Documents 1, 2, 3, 4, 5 and 6 are held electronically on 'SETA's Secured Server' under a 'Quality Management' server, which is managed primarily by the Centre Compliance Manger and only accessible by the Chief Executive Officer, the Chief Operating Officer and the Business Services Manager. Erasure will take place by the Centre Compliance Manager following '**6.10.7 - Data Erasure Model**' after a period of 1 month following a staff member's employment having ceased.

Documents 6 and 7 are held electronically on 'SETA's Secured Server' under an 'Internal Quality Assurance' server, which is only accessible to said Assessor/Internal Quality Assurer, the Chief Operating Officer, the Centre Compliance Manager and the Apprenticeship Services Manager. This Data is shared with EAL, City & Guilds and

the ECITB via their own electronic systems and in compliance with their own Data protection protocols. These will be erased after a period of 3 years following the date of Internal Quality Assurance by the Centre Compliance Manager by following '**6.10.7 - Data Erasure Model**'.

5.5 Employers

Employers with apprentices or learners attending SETA will have both personal data, including special categories of personal data collected and held on various sources as set out in '**6.10.6 Electronic and Paper-based Records Access Control, Rules and Rights Policy and Procedure**'.

SETA requires Data to be collected either via SETA's own Application forms or those generated by the Awarding Bodies and Organisations for Registration and Certification purposes. This Data will be shared electronically with the Awarding Bodies and Organisations in line with their own Data sharing protocols for Qualification Registration and Certification purposes only.

All completed paperwork and documents are scanned and held electronically on SETA's secured Server for a period of 6 years. They will be erased after this period by the Administration team. The Administration team will destroy all completed paperwork and documents once they have been processed electronically by following '**6.10.7 - Data Erasure Model**'.

5.6 Subcontractors

SETA does not deal with any subcontractor arrangements.

6. Procedures

6.1 Data Subject Erasure Request and Procedure

Please see procedure '**CEN-029 - Privacy Policy'** for details on how SETA will deal with this.

6.2 Staff Training

All SETA staff were briefed on the new Data Protection Act 2018 during an inset day during July 2018 by the Centre Compliance Manager. All new staff receive this training as part of their staff induction. Refresher training is also organised annually, and new updates to policies, procedures, the Data Protection Act 2018 and the UK GDPR will be communicated by the Centre Compliance Manager during SETA's monthly staff briefings.

6.3 Data Subject Access Request Procedure

Please see procedure '**CEN-029 - Privacy Policy'** for details on how SETA will deal with this.

6.4 Privacy Notice and Procedure

Please see procedure '**CEN-029 - Privacy Policy'** for details on how SETA will deal with this.

6.5 Retention of Records Procedure

All SETA's records, whether paper-based or digital, are subject to the retention requirements of this procedure, which is set out in '**CEN-022 - Document and Records Retention**' and it's **Annex A**. Please refer to this for information.

6.6 Data Subject Consent Procedure

Please see procedure '**CEN-029 - Privacy Policy'** for details on how SETA will deal with this.

6.7 Data Subject Change Request Procedure

Please see procedure '**CEN-029 - Privacy Policy'** for details on how SETA will deal with this.

6.8 Complaints Procedure

This forms part of SETA's '**COM-015 - Handling Complaints**' procedure. Please see this for further details.

6.9 Data Breaches

The ICO defines a Personal Data Breach as:

'A security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals'.

SETA takes the security of any Data collected, including personal and sensitive personal information very seriously. When such a security incident takes place, SETA will establish as quickly as possible whether a personal Data breach has occurred and, if so, take the necessary corrective action to address it.

SETA has a duty to report certain types of a Data breaches to the ICO, which will be carried out by both the Data Protection Officer, the Chief Executive Officer and the Chief Operating Officer within 72 hours of becoming aware of the breach, where feasible. If at the time of the breach SETA does not have all the details to submit to the ICO, SETA will notify the ICO within 72 hours of becoming aware of the breach explaining that SETA does not yet have all the relevant details, but it is expect SETA will have the results of the investigation within a few days. Once our investigation uncovers details about the incident, we will give the ICO the information about the breach immediately.

Examples of Data breaches that could occur at SETA are as follows:

- *access to SETA's documents and systems by unauthorised personnel*
- *deliberate or accidental action by a controller or processor*
- *sending personal Data to an incorrect recipient*
- *a laptop or PC containing personal Data being lost or stolen*
- *a memory stick or external hard drive containing personal Data being lost or stolen*
- *alteration of personal Data without permission*
- *loss or corruption of personal Data*
- *documents containing personal details left on the photocopier*
- *sharing of e-mail address without use of BCC*

6.9.1 Breach Notification and Investigation Procedure

When a personal Data breach has occurred, SETA's Data Protection Officer and Chief Operating Officer will establish the likelihood and severity of the resulting risk to people's rights and freedoms by carrying out an investigation and recording it on a 'Breach Investigation Form' **(Please see Annex E)**, along with the ICO's online tool 'Self-assessment for data breaches' at https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/. If it is likely that there will be a risk, SETA will notify the ICO. If it is unlikely, SETA will not report it and it will be recorded and documented on a 'Non Risk Breach Recording From' **(Please see Annex F)** so SETA can justify this decision.

The Centre Compliance Manager will report a breach to the ICO by either calling them on 0303 123 1113 or providing them with a completed 'Report a personal data breach' form **(Please see Annex G)**, via e-mail to The Data Protection Officer will e-mail the form to icocasework@ico.org.uk

SETA will report the breach to the persons to which the breach affects by written letter **(Please see Annex H)** which includes the following information:

- *a description of the nature of the personal Data breach*
- *the name and contact details of SETA's 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 where appropriate, a description of the measures taken to mitigate any possible adverse effects*

Once the breach notification and investigation procedure has been completed, the Data Protection Officer will liaise with the ICO and instigate any corrective action that must be taken.

All UK GDPR activity and breaches will be recorded on the 'UK GDPR Incident Log' which is found in the folder entitled '39. Quality UK GDPR' on the secured Quality Management server.

6.10 Information Security

6.10.1 Secure Disposal of Storage Media

All Staff desktop and Laptop computers at SETA are purchased as assets through an IT subcontractor, 'NetPrimates' and are currently either 'HP Prodesk' tower systems or 'HP Probook' laptop computers managed by 'NetPrimates'. When computers reach the end of their life, they are disposed of by NetPrimates using their own protocols, who in turn would supply a certificate of destruction for the internal Hard-Disk drive of the computers as proof Data on them is destroyed adequately.

Hard-Disk drives can also be taken away by the same contracting company that securely destroys the centres confidential waste, and will supply a certificate of destruction upon request.

All SETA's staff have a computer containing an officially licensed copy of Microsoft Windows 10 Professional operating system installed on their hard drive and their own secured access area on the server. They are encouraged to store their teaching notes, lessons plans and daily work on their server area, rather than their computers hard drive, and not to store anything that contains Personal or Sensitive Personal Data.

Managers and Officers who have access to electronic personal and special category Data will use the secure storage area for their files. If the server needs to be replaced, the drive will be taken away and disposed of by SETA's IT subcontractor using their own protocols and replaced with a brand new drive.

Tape Drives, 3.5" Floppy Disks, 5.25"Floppy Disks, Zip-Drives, CD-ROM's and DVD-ROM's are not in use for storage at SETA. USB Flash drives are encouraged for use, but not for storing electronic personal and special category Data, or backups.

6.10.2 Wireless Computer Security Procedure

Please refer to section 15 and 16 of procedure **'CEN-020 - Information Technology'**.

6.10.3 Physical Entrance, Controls and Security Areas

SETA's officers are positioned in an office on the upper mezzanine in 1st Avenue. Access to this area is for authorised members of staff only, and staff located there use a designated printer/photocopier incorporating a 'locked' printing method. This eliminates documents holding personal and sensitive personal Data being left on the printer/photocopier for unauthorised staff to see. Each staff member is required to physically enter a username and password in to the printer/photocopier in order to access their documents. All other staff use a different printer/photocopier located in the staff room in another part of the building.

Staff in 2nd Avenue have access to a printer/photocopier located in the front of the building that also incorporates the 'locked' printing method.

SETA's 1st Avenue main entrance and offices at the front of the building have a restricted 'Swipe Card' entry system and is for those staff having authorisation.

Both SETA buildings enjoy a CCTV system which has 24 cameras placed at various points around the centre in 1st Avenue and one in reception in the building located in 2nd Avenue. One particular camera in SETA's 1st Avenue site is located facing entry to the access controlled records storage room, where various portfolios for learners work is kept secure.

6.10.4 Document Control Procedure

Please see procedure '**CEN-031 – Document Control'** for details on how SETA will deal with this.

6.10.5 Electronic User Access Management

The 'Apprenticeship Training and Assessment Server' is only accessible to the staff identified in **Annex I, Section 1**

The 'Internal Quality Assurance' Server is only accessible to the staff identified in **Annex I, Section 2**

The 'apprenticeships' Server is only accessible to the staff identified in **Annex I, Section 3**

Please see Section 4 of '**COM-021 - Apprenticeship Standards Recruitment and Sign-up**' for the latest information on access rights for the 'Apprenticeships' server

Please see Annex N for Server groups and permissions across the centre.

6.10.6 Electronic and Paper-based Records Access Control, Rules and Rights Policy and Procedure

Employers with apprentices at SETA enrolled before September 2017 will have paper-based documents held in an employer file and their respective apprentice's files, which are located in a locked filing cabinet and kept by the Apprenticeship Services Manager. This will contain a copy of the following documents:

- *Learner workplace reviews*
- *Learner cause for concerns*
- *Learner disciplinaries*
- *SETA application form*
- *SETA enrolment form*
- *agreement on acceptable behaviour form*
- *certificate copies*
- *CV*
- *ILR form*
- *ILP*
- *PLR*
- *Statement of School results*
- *Student photo video consent form*
- *Certificate registration and claims form*
- *Qualification Registration confirmation*
- *Certificate of employers' Public Liability Insurance*
- *Certificate of employers' Liability Insurance*
- *Employer Incentive Claim Form*
- *Contract of employment*
- *Paper based NAS Grant Application form*

Employers with apprentices at SETA enrolled after September 2017 will have electronic documents held on the secured server with restricted access and in line with '**6.10.5 Electronic User Access Management**'. This will contain a copy of the following documents:

- *Learner workplace reviews*
- *Learner cause for concerns*

- *Learner disciplinaries*
- *SETA application form*
- *SETA enrolment form*
- *Agreement on acceptable behaviour form*
- *Certificate copies*
- *CV*
- *ILR form*
- *ILP*
- *PLR*
- *Statement of School results*
- *Student photo video consent form*
- *SETA commitment statement form*
- *Certificate registration and claims form*
- *Qualification Registration confirmation*
- *Certificate of employers' Public Liability Insurance*
- *Certificate of employers' Liability Insurance*
- *SETA commitment statement form*
- *Employer Incentive Claim Form*
- *Contract of employment*
- *Job description and training requirements form*
- *SETA commitment statement form*

Learners NVQ, Technical Certificate Portfolios, Assessment and Internal Quality Assurance records relating to EAL and Pearson Awarding bodies are held in a designated locked archive room.

Historically, NVQ Assessors and Apprenticeship review staff have taken paper-based files out to the workplace when visiting Apprentices and Learners on NVQ programmes to refer to. Carbon-copy review sheets in physical form were also completed and kept in these files; introduction of the electronic system has eliminated the need for paper-based files.

6.10.7 Data Erasure Model

Electronic Data will be erased through the computer operating system, namely Microsoft Windows 10 Professional and will be carried out by the Data processor at the designated set time period, when the Data is no longer required. Because the Data is located on a secured server, the Data will be erased at the time of erasure with no chance of it being retrieved via a 'Recycle Bin'. The Data Protection Officer will manage erasure in conjunction with the Data Processors when an 'Erasure Request' is made.

Buildings in both 1st and 2nd Avenue have a photocopier that is used for scanning purposes. All documents scanned are saved to a secured server and are automatically erased at the end of each day.
Paper based documents will be either:

- *shredded via SETA's cross shredding machine and put in bags with normal rubbish*
- *placed into the white bag which is collected and destroyed by a sub-contracting company*

This will be carried out by the Data processor at the designated set time period when the Data is no longer required. The Data Protection Officer will manage erasure in conjunction with the Data Processors when an 'Erasure Request' is made.

The Business Services Manager will arrange for the secure disposal and removal of paper-based documents that require secure shredding.

Due to the nature of SETA's business, certain Data cannot be erased and will need to be kept for legitimate reasons. These are as follows:

- *Learners on apprenticeships* **(Please see Annex J, Section 1)**
- *Learners who have completed an apprenticeship and left SETA* **(Please see Annex J, Section 2)**
- *SETA staff* **(Please see Annex J, Section 3)**
- *Commercial learners* **(Please see Annex J, Section 4)**
- *Subcontractors* **(Please see Annex J, Section 5)**
- *Employers* **(Please see Annex J, Section 6)**

6.10.8 Laptop's Used Externally Off-Site

Apprentices and Learners studying under programmes of training and Assessment with SETA are visited regularly in the workplace and electronic reviews are carried out by staff on laptops. Laptops are also taken out of SETA for use by other staff for various work reasons. Therefore, these Laptops are encrypted via 'Microsoft Bitlocker' to ensure if they are lost, stolen or misplaced, information cannot be accessed form them by any unauthorised persons.

6.11 Internal Audit Procedure

SETA's Data Protection Officer performs annual audits in each area of SETA's Offices in both 1st Avenue and 2nd Avenue, and complies the following information in a spreadsheet **(Please see Annex P)**:

- *The area of the audit*
- *What Data is collected*
- *Where the Data is collected*
- *Where the Data is stored*
- *The function/reason for every piece of Data collected*
- *Where the Data originated from*
- *How the Data is protected and documented*
- *How long the Data will be kept*
- *The process if someone asks for their Data to be removed from SETA's records*
- *Who the Data be shared with*

If areas are found that could potentially be a breach, it is actioned on the spreadsheet, including who will do what and when to rectify the risk.

6.12 Supply of Documents and Encryption

SETA subscribes to the Barracuda e-mail encryption service, where all staff are able to send encrypted e-mails through their Microsoft Office 365 accounts, without the need to supply a password. This should be used in all cases where attachments containing personal and special category data are sent to customers.

If it is not possible to use the Barracuda system for any reason, 'Foxit Phantom' PDF writer and '7zip' software should be used to encrypt document attachments to send and receive e-mails via 128AES password encryption.

Personal data or special category data must never be communicated within the body of an e-mail.

All single documents containing Personal and Sensitive Personal Data that is distributed via e-mail as specified below should have a password if Barracuda is not used:

- *Microsoft Word*
- *Microsoft Excel*
- *Microsoft PowerPoint*
- *Microsoft Access*
- *Foxit Phantom PDF*

- *ASCII and Text Files*

When more than one document is required to be distributed, they will be compressed together using 7zip software and encrypted as a 128AES password encrypted ZIP file.

Please see **CEN-020 - Information Technology, Section 20** for SETA's password policy.

In this case, SETA assigns an employer with a password, so all documents sent to the employer via SETA will consist of the same password that the recipient will be made aware of. A spreadsheet consisting of this Data is avail be on SETA's shared server in password-encrypted format which is only made available to the following staff:

- *Chief Executive Officer*
- *Chief Operating Officer*
- *Centre Compliance Manager*
- *Apprenticeship Services Manager*
- *Lead Instructor*
- *Engagement Services Manager*
- *Workplace Assessment Team*
- *Administration Team*

Once a document has been encrypted using a password, it will be sent to the third party via e-mail with the password sent in a separate e-mail.

When there is a need for documents to be returned from the third party, SETA will request the recipient to send the documents back via e-mail using the same protocol, which under the UK GDPR is the responsibility of the third party.

It is however, highly recommended that the Barracuda system is used wherever possible.

6.13 Data Portability Procedure

Article 20 of Regulation (EU) 2016/679 states '*The Data subject shall have the right to receive the personal Data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those Data to another controller without hindrance from the controller to which the personal Data have been provided*'.

6.13.1 Apprentices and Their Employers

SETA's uses PICSWEB, an online LMS system portal provided by Pellcomp. It has the option of being able to export a Learner and Employer data as part of the software's 'UK GDPR Tools'. The encrypted exporting of data will be instigated by the Data Protection Officer when a request is made by completing a 'Data Subject Portability Request' form **(Please see Annex K)**, or by asking a member of staff, who in turn will refer the person to the Data Protection Officer, who will process the request.

Apprentices and their Employers who enrolled on an apprenticeship on or after September 2017 will have copies of their files held electronically on SETA's secured apprenticeships Server. These files can be encrypted in to a Zip file and given to them electronically along with an export form generated via the PICSWEB LMS.

Apprentices and their Employers who enrolled on an apprenticeship prior to September 2017 will have all of their details held in a paper based filing system. These documents will be converted in to electronic files and handed over to them in an encrypted Zip file either via supplied USB media or e-mail.
Apprentices and their Employers will be given their Data in portable format, once they have left their apprenticeship programmes, or have severed their ties to SETA if requested. It will not be erased from SETA's

systems, until the correct time period has passed or if a Data Subject Erasure Request and Procedure as specified in '**6.1 Data Subject Erasure Request and Procedure**' is followed.
All encryption will follow that as described in '**6.12 Supply of Documents and Encryption**'.
SETA will not charge for this service.

Data held on/via Awarding Bodies and Awarding Organisations systems is not part of SETA's Data storage facility, so SETA is not able to provide portable Data from them.

6.13.2 SETA employees
Paper-based documents will be converted in to electronic files and handed over to the employer in an encrypted Zip file either via supplied USB media or e-mail.

6.13.3 Commercial learners
Paper-based documents will be converted in to electronic files and handed over to the learner in an encrypted Zip file either via supplied USB media or e-mail.

6.14 Data Protection Impact Assessment Procedure (DPIA)
SETA will carry out a DPIA if it is believed that processing Data is likely to result in a high risk to its customers.

SETA's does not engage in projects outside its main scheme of training and assessing commercial learners and apprentices. Therefore, all processing is deemed to be a repeat process.

SETA will carry out a DPIA in line with current ICO recommendations and using their adopted template **(Please see Annex L)** if any of the following conditions should arise:

- *Use of new technologies*
- *Processing Biometric or genetic Data*
- *Combining, comparing or matching Data from multiple sources*
- *Processing personal Data which could result in a risk of physical harm in the event of a security breach*
- *Processing of sensitive Data or Data of a highly personal nature*
- *Processing on a large scale*
- *Processing of Data concerning vulnerable Data subjects*
- *Innovative technological or organisational solutions*

6.14.1 Data Protection Impact Assessment Register
Annex M and Q contain information on areas SETA has carried out Data Protection Impact Assessments.

6.15 Schedule of Authorities, Key Suppliers and Customers
Apprentices, employers and other learners who sign up for training with SETA are considered to be SETA's customers.

All Data Protection agreements received and processed by SETA's customers are held electronically on SETA's secured shared server located within the folder entitled '39. Quality Data Protection'. It is the responsibility of the Data Protection Officer to maintain this folder.

6.15.1 Employers using SETA to Train their Apprentices and Learners
SETA believes that it is the responsibility of the employer to draw up Data Protection agreement between SETA and themselves describing how SETA should be processing and managing their Data.

SETA has a responsibility to communicate with the employer's information on how SETA complies with the Data Protection Act 2018 and it shall do so as highlighted in sections 4 and 5.

6.15.2 Privately Paying learners using SETA to Train Themselves

SETA has a responsibility to communicate with the learner information on how SETA complies with the Data Protection Act 2018 and it shall do so as highlighted in sections 4 and 5.

6.15.3 Suppliers

SETA's suppliers consist only of Awarding Bodies, Awarding Organisations, and Government Bodies, and on some occasions, employers actively seeking an apprentice using SETA's Recruitment service. SETA has no other suppliers. Please see Section 4 for further details on who/how it complies with the Data Protection Act 2018

6.16 Clear Desk Policy

To improve the security and confidentiality of information, SETA has adopted a clear desk policy for desks and computer workstations. This ensures that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device is properly locked away or disposed of when a desk or workstation is not in use.

This will reduce the risk of unauthorised access, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended.

This following guidelines applies to all full time, part time, permanent, temporary and contracted staff working at the Centre:

Whenever a workstation or desk is unoccupied for an extended period of time, the following will apply:

- *All sensitive and confidential paperwork must be removed from the desk and locked in a drawer or filing cabinet. This includes:*
    - *Mass storage devices such as CDs, DVDs, and USB drives*
    - *Post-it notes containing names, phone numbers, user-names and passwords*
- *All waste paper which contains sensitive or confidential information must be placed in the designated confidential waste sacks or shredded manually. Under no circumstances should this information be placed in regular waste paper bins*
- *Computer workstations must be locked when the desk is unoccupied and completely shut down/logged-off at the end of the working day*
- *Laptops, tablets, and other hardware devices must be removed from the desk and locked in a drawer or filing cabinet*
- *Keys for accessing drawers or filing cabinets should not be left unattended at a desk*

Printers and fax machines should be treated with the same care under this policy:

- *Any print jobs containing sensitive and confidential paperwork should be retrieved immediately. When possible, the "Locked Print" functionality should be used*
- *All paperwork left over at the end of the work day will be properly disposed of*

These guidelines require the participation of staff and contractors to be successful. Any employee or contractor found to have violated this policy may be subject to disciplinary action.

6.17 International Data

SETA stores its Data on servers in the United Kingdom. No Data is held or transferred internationally.

It may be possible that certain Certification for courses is sent to Countries within the EU, which would be carried out under the normal postal system for post sent overseas.

SETA does not operate outside the EU.

6.18 Server Backup

All data on SETA's Server is backed up to an external source on a daily basis, with a 30 day retention period; data is encrypted in transit and at rest in a UK based datacenter.

6.19 Network Protection

SETA's networks are protected by a Security Appliance with protection against new and evolving network threats, including advanced malware and ransomware. We have a multi-layer approach on End point protection offering protection against Malware, Ransomware and Online based threats.

7. Review

This policy will be reviewed annually by the Data Protection Officer, the Chief Executive Officer and the Chief Operating Officer.

SETA is in communication with the ICO and will update this policy as and when new information is received.

8. Contact

SETA's Data Protection Officer can be contacted at dataprotection@seta-training.co.uk or on (023) 8087 8307.

Further information on Data Protection and the UK GDPR can be found at https://ico.org.uk/

The Data Protection Act 2018 can be viewed at http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

SETA is registered with the ICO with number Z5243133.

Risk Management

DATA being accessed by unauthorised people through poor security				
Area Considered 'At Risk'	**'unauthorised' Definition**	**Risk of Breach**	**Risk Reasoning**	**Impact of Breach**
Apprenticeship and Employer DATA collected is stored on a secured server and in a locked cabinet held by the Apprenticeship Services Manager.	Apprentices	Low	• No Access to Apprentices • Room is unlocked, but files under lock and key • Apprentices unaware of what is held in the filing cabinets • Filing cabinets could be left unlocked • Apprentices unlikely to want access to others DATA • Apprentices unlikely to want to steal DATA held on others • Apprentices in and around SETA for long periods of time will be aware of SETA's security measures • Shared Drive only accessible via staff 'SETA Private' network.	• Personal DATA could be taken and passed on to a third party • Risk of finding out where other Apprentices live • Risk of finding out other Apprentices learning difficulties and/or disabilities • Risk of finding out Parents/NOK names and address
	Staff	Medium	• Limited staff access • Some staff unaware of what is held in the filing cabinets • Room is unlocked, but files under lock and key • Filing cabinets could be left unlocked • Staff unlikely to want access to others DATA • Staff unlikely to want to steal DATA held on others • Staff are DBS checked and employed in to a trustworthy position. • Certain Shared Drive areas only accessible to some limited staff	• Personal DATA could be taken and passed on to a third party • Risk of finding out where Apprentices live • Risk of finding out Parents/NOK names and address
	Commercial Learners	Low	• No Access to Learners • Learners unaware of room and contents of filing cabinets • Room is unlocked, but files under lock and key • Filing cabinets could be left unlocked • Commercial Learners unlikely to want access to others DATA • Commercial Learners unlikely to want to steal DATA held on others • Commercial Learners are in and around SETA for short periods of time and are not usually left unaccompanied by a member of staff • Shared Drive only accessible via staff 'SETA Private' network.	• Personal DATA could be taken and passed on to a third party • Risk of finding out where Apprentices live • Risk of finding out Apprentices learning difficulties and/or disabilities • Risk of finding out Parents/NOK names and address
	Visitors	Medium	• No Access to Visitors • Visitors unaware of room and contents of filing cabinets • Room is unlocked, but files under lock and key • Filing cabinets could be left unlocked • Visitors are in and around SETA for short periods of time and are not left unaccompanied by a member of staff • Shared Drive only accessible via staff 'SETA Private' network.	• Personal DATA could be taken and passed on to a third party • Risk of finding out where Apprentices live • Risk of finding out Apprentices learning difficulties and/or disabilities • Risk of finding out Parents/NOK names and address

Risk Management

Commercial Course DATA collected is stored on a secured server and in locked filing cabinets in SETA First Avenue which has limited access by staff (Please see 6.10.5 and 6.10.6)	Apprentices	Low	• No Access to Apprentices Room is accessible to Staff only • Room could be left unmanned • Apprentices unaware of what is held in the filing cabinets • Filing cabinets could be left unlocked • Apprentices unlikely to want access to others DATA • Apprentices unlikely to want to steal DATA held on others • Apprentices in and around SETA for long periods of time will be aware of SETA's security measures • Shared Drive only accessible via 'SETA Private' network.	• Personal DATA could be taken and passed on to a third party • Risk of finding out where Learners live • Risk of finding out Parents/NOK names and address • Risk of finding out Learners learning difficulties and/or disabilities
	Staff	Medium	• Limited staff access • Room could be left unmanned • Some staff unaware of what is held in the filing cabinets • Filing cabinets could be left unlocked • Staff unlikely to want access to others DATA • Staff unlikely to want to steal DATA held on others • Staff are DBS checked and employed in to a trustworthy position. • Certain Shared Drive areas only accessible to some limited staff	• Personal DATA could be taken and passed on to a third party • Risk of finding out where Learners live • Risk of finding out Parents/NOK names and address
	Commercial Learners	Low	• No Access to Learners. Room is accessible to Staff only • Learners unaware of contents of filing cabinets • Room could be left unmanned, but files under lock and key • Filing cabinets could be left unlocked • Learners are in and around SETA for short periods of time and are not left unaccompanied by a member of staff • Shared Drive only accessible via staff 'SETA Private' network.	• Personal DATA could be taken and passed on to a third party • Risk of finding out where Learners live • Risk of finding out Parents/NOK names and address • Risk of finding out Learners learning difficulties and/or disabilities
	Visitors	Medium	• No Access to Visitors. Room is accessible to Staff only • Visitors unaware of room and contents of filing cabinets • Room could be left unmanned, but files under lock and key • Filing cabinets could be left unlocked • Visitors are in and around SETA for short periods of time and are not left unaccompanied by a member of staff • Shared Drive only accessible via staff 'SETA Private' network.	• Personal DATA could be taken and passed on to a third party • Risk of finding out where Learners live • Risk of finding out Parents/NOK names and address • Risk of finding out Learners learning difficulties and/or disabilities
Staff DATA collected is stored on a secured server and in a locked filing cabinet that has limited access by staff (Please see 5.4)	Apprentices	Low	• No Access to Apprentices • Staff computer could be left unmanned – *2min screensaver implemented* • Apprentices unaware of what is held on the server • Filing cabinets could be left unlocked • Apprentices unlikely to want access to staff DATA • Apprentices unlikely to want to steal staff held on others	• Personal DATA could be taken and passed on to a third party • Risk of finding out where Staff live • Risk of finding out NOK names and address • Risk of finding out Staff history • Risk of DBS DATA Breach

			• Apprentices in and around SETA for long periods of time will be aware of SETA's security measures • Shared Drive only accessible via 'SETA Private' network.	
	Staff	Low	• No Access to unauthorised staff • Managers computers could be left unmanned – *2min screensaver implemented* • Some staff unaware of what is held on the server • Filing cabinets could be left unlocked • Staff unlikely to want access to staff DATA • Staff unlikely to want to steal staff held on others • Staff are DBS checked and employed in to a trustworthy position • Staff in and around SETA for long periods of time will be aware of SETA's security measures • Shared Drive only accessible via 'SETA Private' network. • Some files and folders have limited access	• Personal DATA could be taken and passed on to a third party • Risk of finding out where other Staff live • Risk of finding out NOK names and address • Risk of finding out Staff history • Risk of DBS DATA Breach
	Commercial Learners	Low	• No Access to Commercial Learners • Staff computer could be left unmanned – *2min screensaver implemented* • Commercial Learners unaware of what is held on the server • Filing cabinets could be left unlocked • Commercial Learners unlikely to want access to staff DATA • Commercial Learners unlikely to want to steal staff held on others • Commercial Learners are in and around SETA for short periods of time and are not left unaccompanied by a member of staff • Shared Drive only accessible via 'SETA Private' network.	• Personal DATA could be taken and passed on to a third party • Risk of finding out where Staff live • Risk of finding out NOK names and address • Risk of finding out Staff history • Risk of DBS DATA Breach
	Visitors	Low	• No Access to Visitors • Visitors unaware of office and contents of filing cabinets • Room could be left unmanned, but files under lock and key • Staff computer could be left unmanned – *2min screensaver implemented* • Filing cabinets could be left unlocked • Visitors are in and around SETA for short periods of time and are not left unaccompanied by a member of staff • Shared Drive only accessible via staff 'SETA Private' network.	• Personal DATA could be taken and passed on to a third party • Risk of finding out where Staff live • Risk of finding out NOK names and address • Risk of finding out Staff history • Risk of DBS DATA Breach
Subcontractors DATA collected is stored on a secured server and in a locked filing cabinet that has limited access by staff (Please see 4.6)	Apprentices	Low	• No Access to Apprentices • Staff computer could be left unmanned – *2min screensaver implemented* • Apprentices unaware of what is held on the server • Filing cabinets could be left unlocked • Apprentices unlikely to want access to subcontractor DATA	• Personal DATA could be taken and passed on to a third party

			• Apprentices unlikely to want to steal subcontractor DATA • Apprentices in and around SETA for long periods of time will be aware of SETA's security measures • Shared Drive only accessible via 'SETA Private' network.	
	Staff	Low	• No Access to unauthorised staff • Managers computers could be left unmanned – *2min screensaver implemented* • Some staff unaware of what is held on the server • Filing cabinets could be left unlocked • Staff unlikely to want access to subcontractor DATA • Staff unlikely to want to want to steal subcontractor DATA • Staff in and around SETA for long periods of time will be aware of SETA's security measures • Staff are DBS checked and employed in to a trustworthy position • Shared Drive only accessible via 'SETA Private' network. • Some files and folders have limited access	• Personal DATA could be taken and passed on to a third party
	Commercial Learners	Low	• No Access to Commercial Learners • Staff computer could be left unmanned – *2min screensaver implemented* • Commercial Learners unaware of what is held on the server • Filing cabinets could be left unlocked • Commercial Learners unlikely to want access to subcontractor DATA • Commercial Learners unlikely to want to steal subcontractor DATA • Commercial Learners are in and around SETA for short periods of time and are not left unaccompanied by a member of staff • Shared Drive only accessible via 'SETA Private' network.	• Personal DATA could be taken and passed on to a third party
	Visitors	Low	• No Access to Visitors • Visitors unaware of office and contents of filing cabinets • Room could be left unmanned, but files under lock and key • Staff computer could be left unmanned – *2min screensaver implemented* • Filing cabinets could be left unlocked • Visitors are in and around SETA for short periods of time and are not left unaccompanied by a member of staff • Shared Drive only accessible via staff 'SETA Private' network.	• Personal DATA could be taken and passed on to a third party
E-mails containing documents that contain Personal and Sensitive Personal DATA sent via e-mail will be encrypted (Please see 5.12)	Apprentices	Low	• No Access to Apprentices • Staff computer could be left unmanned – *2min screensaver implemented* • Apprentices in and around SETA for long periods of time will be aware of SETA's security measures	• Personal DATA could be taken and passed on to a third party

			• Shared Drive only accessible via 'SETA Private' network • ZIP, PDF, XLSX, DOCX and PPTX files to be sent to employers via password encryption.	
	Staff	Low	• All Computers have password protection • No sharing of Computers allowed • All staff have individual access to Outlook 365 Accounts • Staff computer to have 2min screensaver activated • Staff are DBS checked and employed in to a trustworthy position • Shared Drive only accessible via 'SETA Private' network • ZIP, PDF, XLSX, DOCX and PPTX files to be sent to employers via password encryption by designated managers only • No e-mails are stored on the shared server	• Personal DATA could be taken and passed on to a third party
	Commercial Learners	Low	• No Access to Commercial Learners • Staff computer could be left unmanned – *2min screensaver implemented* • Commercial Learners are in and around SETA for short periods of time and are not left unaccompanied by a member of staff • Shared Drive only accessible via 'SETA Private' network. • ZIP, PDF, XLSX, DOCX and PPTX files to be sent to employers via password encryption, so interception would not be easy.	• Personal DATA could be taken and passed on to a third party
	Visitors	Low	• No Access to visitors • Staff computer could be left unmanned – *2min screensaver implemented* • Visitors are in and around SETA for short periods of time and are not left unaccompanied by a member of staff • Shared Drive only accessible via 'SETA Private' network. • ZIP, PDF, XLSX, DOCX and PPTX files to be sent to employers via password encryption, and those know are e-mailed and aware of password so interception would not be easy.	• Personal DATA could be taken and passed on to a third party
Registration and Certification of courses is controlled by Awarding Bodies and Awarding Organisations own secured online portals, which has limited staff access controlled by SETA's Quality & Compliance Manager	Apprentices	Low	• No Access to Apprentices • Staff computer could be left unmanned – *2min screensaver implemented* • Apprentices in and around SETA for long periods of time will be aware of SETA's security measures	• Personal DATA could be taken and passed on to a third party
	Staff	Low	• Limited staff access to systems • Managers computer could be left unmanned – *2min screensaver implemented* • Staff are DBS checked and employed in to a trustworthy position	• Personal DATA could be taken and passed on to a third party

Risk Management

			• Apprentices in and around SETA for long periods of time will be aware of SETA's security measures	
	Commercial Learners	Low	• No Access to Commercial Learners • Staff computer could be left unmanned – *2min screensaver implemented* • Commercial Learners are in and around SETA for short periods of time and are not left unaccompanied by a member of staff	• Personal DATA could be taken and passed on to a third party
	Visitors	Low	• No Access to Visitors • Staff computer could be left unmanned – *2min screensaver implemented* • Visitors are in and around SETA for short periods of time and are not left unaccompanied by a member of staff	• Personal DATA could be taken and passed on to a third party
SETA's MIS and CRM containing Learner and Employer DATA has limited staff access controlled by SETA's Centre Compliance Manager	Apprentices	Low	• No Access to Apprentices • Staff computer could be left unmanned – *2min screensaver implemented* • Apprentices in and around SETA for long periods of time will be aware of SETA's security measures	• Personal DATA could be taken and passed on to a third party • Risk of finding out where other Apprentices live • Risk of finding out other Apprentices learning difficulties and/or disabilities • Risk of finding out Parents/NOK names and address
	Staff	Low	• Limited staff access to systems • Managers computer could be left unmanned – *2min screensaver implemented* • Staff are DBS checked and employed in to a trustworthy position • Apprentices in and around SETA for long periods of time will be aware of SETA's security measures	• Personal DATA could be taken and passed on to a third party • Risk of finding out where Apprentices live • Risk of finding out Parents/NOK names and address
	Commercial Learners	Low	• No Access to Commercial Learners • Staff computer could be left unmanned – *2min screensaver implemented* • Commercial Learners are in and around SETA for short periods of time and are not left unaccompanied by a member of staff	• Personal DATA could be taken and passed on to a third party • Risk of finding out where Apprentices live • Risk of finding out Apprentices learning difficulties and/or disabilities • Risk of finding out Parents/NOK names and address
	Visitors	Low	• No Access to Visitors • Staff computer could be left unmanned – *2min screensaver implemented* • Visitors are in and around SETA for short periods of time and are not left unaccompanied by a member of staff	• Personal DATA could be taken and passed on to a third party • Risk of finding out where Apprentices live • Risk of finding out Apprentices learning difficulties and/or disabilities • Risk of finding out Parents/NOK names and address

Risk Management

Contacting the incorrect person or an incorrect person being given the wrong information	Anyone	Medium	• Administration staff sending out the wrong documents to the wrong person - *ZIP, PDF, XLSX, DOCX and PPTX files to be sent to employers via password encryption, so the incorrect file would not be openable.* • 'vishing' and/or 'phishing' could happen where staff are tricked into giving away information over the phone or by email – *no information will be given out over the telephone. A written request in line with SETA's Privacy Policy is required.*	• Personal DATA could be taken and passed on to a third party
Staff working at home	Anyone	Medium	• Office 365 e-mail client in use will be web-based and only as secure as the personal computers Wi-Fi and security software not regulated by SETA's IT Department • SETA Laptops in use will follow security protocols regulated by SETA's IT Department but will be connected via staffs own personal Wi-Fi connection • Computer used at home could be left unlocked and open to other family members – *2min screensaver implemented* • Laptop maybe mislaid on route to and from SETA's premises and home • Laptop could be stolen • Access to SETA's secured server and files not possible from outside of SETA's premises • USB storage devices holding documents maybe mislaid on route to and from SETA's premises and home • USB storage devices holding documents could be stolen • Staff are DBS checked and employed in to a trustworthy position • ZIP, PDF, XLSX, DOCX and PPTX files to be sent to employers via password encryption, so interception would not be easy.	• Personal DATA could be taken and passed on to a third party
Working during meetings and with clients present	Employers	Low	• Notes taken on Laptops or other electronic devices could be seen by those present – *2min screensaver implemented* • Only those authorised would be present at the meeting and therefore party to any information discussed	• Personal DATA could be taken and passed on to a third party
	Apprentices	Low	• Notes taken on Laptops or other electronic devices could be seen by those present • Only those authorised would be present at the meeting and therefore party to any information discussed	• Personal DATA could be taken and passed on to a third party
	Sub-contactors	Low	• Notes taken on Laptops or other electronic devices could be seen by those present • Only those authorised would be present at the meeting and therefore party to any information discussed	• Personal DATA could be taken and passed on to a third party
	Visitors	Low	• Notes taken on Laptops or other electronic devices could be seen by those present	• Personal DATA could be taken and passed on to a third party

			• Visitors are in and around SETA for short periods of time and are not left unaccompanied by a member of staff • Only those authorised would be present at the meeting and therefore party to any information discussed	
	Staff	Low	• Notes taken on Laptops or other electronic devices could be seen by those present • Only those authorised would be present at the meeting and therefore party to any information discussed	• Personal DATA could be taken and passed on to a third party

DATA Processors

SETA has adopted this ICO guidance in general, and DATA Processors have been identified as the following staff:

Position	Work/Responsibilities Involved as a Processor
Tutors and Internal Assessors	Entering Learner DATA in to Reports, Registers and NVQ Assessment Documents
Administrators	Entering DATA in Awarding Bodies/Organisations (City & Guilds, JTL, Pearson, ECITB and NET) Systems for Registration and Claims Purposes
Chief Operating Officer	Entering staff DATA in to online HR Management system and liaison with HR contracting company. Storing Staff DATA in Personnel files
Internal Quality Assurers	Entering Learner DATA in to Reports, Registers, Learner Reviews and NVQ Assessment/IQA Documents
Workplace Assessors	Entering Learner DATA in to Reports, Registers, Learner Reviews and NVQ Assessment/IQA Documents
Chief Executive Officer	Entering staff DATA in to online HR Management system, liaison with HR contracting company, maintaining Personnel files, entering Staff DATA in to the PAYE software/system and entering employer DATA in to SAGE Software for invoicing and remittance
Business Development Manager	Entering Learner DATA in to SETA's MIS and gov.uk Apprenticeships site
Engagements Services Manager	Contacting Schools and their students about SETA projects, entering DATA into timetables, contacting employers about upcoming opportunities and training requirements
Centre Compliance Manager	Entering Learner DATA in Awarding Bodies/Organisations (City & Guilds, EAL and ECITB) Systems for Registration and Claims Purposes and in to Reports, Registers, Learner Reviews and NVQ Assessment/IQA Documents
BTEC/HNC Team Leader	Entering DATA in Awarding Bodies/Organisations (City & Guilds, JTL and NET) Systems for Registration and Claims Purposes and writing progress reports.
Finance Services Manager	Processing Learner and Employer DATA for invoicing purposes, and Staff PAYE
AM2 Examiners	Entering Examination DATA in to the NET online examination system
Apprenticeship Services Manager	Entering Learner DATA in to Reports, Registers, BTEC Assessment Documents. Entering Learner and Employer DATA in to SETA's MIS and Awarding Bodies/Organisations (EAL, Person, SEMTA and ECITB) Systems for Registration and Claims Purposes
Pastoral Support Services and Safeguarding	DATA collection and management of apprentice and staff all matters, Entering personal DATA into the Safeguarding server and maintaining it.

Information Asset Owners

SETA's Information Asset Owners (IAO's) have been identified as the following staff:

Position	Work/Responsibilities Involved as a Controller
Centre Compliance Manager	Learner DATA is entered in to Awarding Body/Organisation systems for registration and claims purpose by Administrators on his behalf. DATA is entered in to learner review forms by the Assessment team and is processed on their behalf.
Administrators	Commercial learner DATA is processed by Administrators on their behalf
Apprenticeship Services Manager	Passes application DATA on to Administrator for entering in PICS MIS on her behalf and passes on information to Assessment team via ILP and Certificates for them to distribute
Finance Manager	Has control over the company's finances

DATA Protection Breach Investigation Form

Date of Breach	Click or tap to enter a date.	**Date of Discovery**	Click or tap to enter a date.	**Date of this Investigation**	Click or tap to enter a date.

DATA Protection Officer	**E-mail Address**	**Telephone No.**
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

Approximate number of individuals concerned	Choose an item.

Categories of Breach		Categories of Data Subjects Affected	
Racial or ethnic origin	☐	SETA Staff	☐
Religious or philosophical beliefs	☐	Commercial Learners	☐
Sexual orientation data	☐	Apprentice Learners	☐
Health data	☐	Apprentice Applicants	☐
Personal identifiers	☐	Employers	☐
Electronic Identifications	☐	Schools	☐
Economic and financial data	☐	Sub-Contractors	☐
Official documents	☐	Not yet known	☐
Criminal convictions and offences	☐	Other (please give details below)	☐
Not yet known	☐	Click or tap here to enter text.	
Other (please give details below)	☐		
Click or tap here to enter text.			

What is the nature of the personal data breach?
Click or tap here to enter text.

How was the breach discovered?
Click or tap here to enter text.

What are the likely consequences of the personal data breach?
Click or tap here to enter text.

Result of Breach		Justification Details
Human Error	☐	Click or tap here to enter text.
A Systemic Issue	☐	

What are the asctions to be taken, or are proposed to be taken to deal with the personal data breach?
(including, where appropriate, the measures taken to mitigate any possible adverse effects)
Click or tap here to enter text.

Non-Risk Breach Recording From

Date of Breach	Click or tap to enter a date.	**Date of Discovery**	Click or tap to enter a date.	**Date of this Investigation**	Click or tap to enter a date.

DATA Protection Officer	**E-mail Address**	**Telephone No.**
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

Approximate number of individuals concerned	Choose an item.

Categories of Breach		Categories of Data Subjects Affected	
Racial or ethnic origin	☐	SETA Staff	☐
Religious or philosophical beliefs	☐	Commercial Learners	☐
Sexual orientation data	☐	Apprentice Learners	☐
Health data	☐	Apprentice Applicants	☐
Personal identifiers	☐	Employers	☐
Electronic Identifications	☐	Schools	☐
Economic and financial data	☐	Sub-Contractors	☐
Official documents	☐	Not yet known	☐
Criminal convictions and offences	☐	Other (please give details below)	☐
Not yet known	☐	Click or tap here to enter text.	
Other (please give details below)	☐		
Click or tap here to enter text.			

What is the nature of the personal data breach?
Click or tap here to enter text.

How was the breach discovered?
Click or tap here to enter text.

What are the likely consequences of the personal data breach?
Click or tap here to enter text.

Result of Breach		Justification Details
Human Error	☐	Click or tap here to enter text.
A Systemic Issue	☐	

What are the asctions to be taken, or are proposed to be taken to deal with the personal data breach?
(including, where appropriate, the measures taken to mitigate any possible adverse effects)
Click or tap here to enter text.

Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. **Please do not include any of the personal data involved in the breach when completing this form**. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

About your report

Please answer the following questions, to help us handle your report efficiently and to better understand our customers.

If you have already spoken to a member of ICO staff about this breach, please give their name:

Report type

- ○ Initial report – report complete
- ○ Follow-up report – report complete
- ○ Initial report – additional information to follow
- ○ Follow-up report – additional information to follow

(Follow-up reports only) ICO case reference:

Reason for report – after consulting the guidance

- ○ I consider the incident meets the threshold to report
- ○ I do not consider the incident meets the threshold to report, however I want you to be aware
- ○ I am unclear whether the incident meets the threshold to report

Size of organisation

- ○ Fewer than 250 staff
- ○ 250 staff or more

Is this the first time you have contacted us about a breach since the GDPR came into force?

- ○ Yes
- ○ No
- ○ Unknown

About the breach

Please describe what happened

Please describe how the incident occurred

How did the organisation discover the breach?

What preventative measures did you have in place?

Was the breach caused by a cyber incident?

- ○ Yes
- ○ No
- ○ Don’t know

When did the breach happen?

Date: Time:

When did you discover the breach?

Date: Time:

Categories of personal data included in the breach (tick all that apply)

- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data
- ☐ Sexual orientation data
- ☐ Gender reassignment data
- ☐ Health data
- ☐ Basic personal identifiers, eg name, contact details
- ☐ Identification data, eg usernames, passwords
- ☐ Economic and financial data, eg credit card numbers, bank details
- ☐ Official documents, eg driving licences
- ☐ Location data, eg coordinates
- ☐ Genetic or biometric data
- ☐ Criminal convictions, offences
- ☐ Other (please give details below)

Please give additional details to help us understand the nature of the personal data included in the breach:

Number of personal data records concerned?

How many data subjects could be affected?

(Cyber incidents only) If the number of data subjects affected is not known, estimate the maximum possible number that could be affected/total customer base

Categories of data subjects affected (tick all that apply)

- ☐ Employees
- ☐ Users
- ☐ Subscribers
- ☐ Students
- ☐ Customers or prospective customers
- ☐ Patients
- ☐ Children
- ☐ Vulnerable adults
- ☐ Other (please give details below)

Describe any detriment to individuals that has arisen so far, or any detriment you anticipate may arise in the future

Is the personal data breach likely to result in a high risk to data subjects?

- ○ Yes
- ○ No
- ○ Not yet known

Please give details

(Cyber incidents only) Recovery time

- ○ We have successfully recovered from the incident with all personal data now at the same state it was shortly prior to the incident
- ○ We have determined that we are able to restore all personal data to the same state it was shortly prior to the incident and are in the process of doing this
- ○ We have determined that we are unable to restore the personal data to the same state it was at shortly prior to the incident, ie backups failed, no

current backup, backup encrypted etc

- ○ We are not yet able to determine if personal data can be restored to the same state it was shortly prior to the incident

Had the staff member involved in this breach received data protection training in the last two years?

- ○ Yes
- ○ No
- ○ Don't know

Please describe the data protection training you provide, including an outline of training content and frequency

(Initial reports only) If there has been a delay in reporting this breach, please explain why

Taking action

Have you taken action to contain the breach or limit its impact? Please describe these remedial actions

Please outline any steps you are taking to prevent a recurrence, and when you expect they will be completed

Describe any further action you have taken, or propose to take, as a result of the breach

Have you told data subjects about the breach?

- ○ Yes – we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects
- ○ Yes – we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway
- ○ No – but we are planning to because we have determined it is likely there is a high risk to data subjects
- ○ No – we determined the incident did not meet the threshold for communicating it to data subjects

Have you told, or are you planning to tell any other organisations about the breach?

- ○ Yes
- ○ No
- ○ Don't know

If you answered yes, please specify

Are you a member of a UK GDPR Code of Conduct or Certification Scheme, as approved and published on the ICO website?

- ○ Yes
- ○ No

If yes:

Please confirm the Code/Scheme name

Are the Code or Scheme's requirements relevant to the breach that has occurred?

- ○ Yes
- ○ No

Have you informed the relevant Monitoring Body or Certification Body?

- ○ Yes
- ○ No

Suspicious websites

If the breach relates to a suspicious website, you can report the website to the National Cyber Security Centre (NCSC). By reporting, you can help stop cyber criminals and protect others online.

The ICO won't see the details of your report to NCSC, so you should make sure you tell us everything we need to know on this form.

Report a suspicious website - NCSC.GOV.UK

About you

Organisation (data controller) name

Registration number

If not registered, please give exemption reason

Business sector

Registered organisation address

Person making this report

In case we need to contact you about this report

Name:

Email:

Phone:

Sending this form

Initial report

If this is your initial report, please send your completed form to icocasework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Follow up report

If this is a follow up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

OR, send by post to:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days to provide information about our next steps. If this is your initial report, we'll give you a case reference number.

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our privacy notice.

Southampton Engineering Training Association Limited

First Avenue, Millbrook, Southampton, SO15 0LJ
Unit 2, Second Avenue, Millbrook, Southampton, SO15 0LP

Telephone: 023 8077 1908 Email: info@seta-training.co.uk
Web: www.setatraining.co.uk

[NAME]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[ADDRESS LINE 3]
[CITY]
[COUNTY]
[POST CODE]

28 March 2023

Dear [NAME]

It is with great regret I must inform you that SETA has suffered a DATA Protection breach and certain DATA SETA holds on you has been compromised.

It was discovered on [DATE], reported to myself on [DATE] and subsequently reported to the Information Commissioners Office (ICO) on [DATE].

- a description of the nature of the personal data breach
- 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
- where appropriate, a description of the measures taken to mitigate any possible adverse effects

If you have any questions, please contact me on (023) 8087 8307 or at dataprotection@seta-training.co.uk and I will be pleased to discuss this further with you.

Yours Sincerely,

Quality & Compliance Manager
(DATA Protection Officer)

Electronic and Paper-Based Records User Access Management

1. The 'Apprenticeship Training and Assessment Server' is only accessible to the following staff:

Position	Requirement	Reason
Workplace Assessors	Access to the 'Assessor Tracking' spreadsheet and Workplace Reviews.	To complete workplace reviews, cause for concerns and Disciplinary documents
Internal Quality Assurers	Access to the 'Assessor Tracking' spreadsheet and Workplace Reviews.	To complete workplace reviews, cause for concerns and Disciplinary documents
Chief Operating Officer	Access to the 'Assessor Tracking' spreadsheet and Workplace Reviews.	To gain current and historical information on Apprentices progress
Centre Compliance Manager	Access to the 'Assessor Tracking' spreadsheet and Workplace Reviews.	To gain current and historical information on Apprentices progress
Apprenticeship Services Manager	Access to the 'Assessor Tracking' spreadsheet and Workplace Reviews.	To gain current and historical information on Apprentices progress
Work-Based Learning Manager	Access to the 'Assessor Tracking' spreadsheet and Workplace Reviews.	To gain current and historical information on Apprentices progress

2. The 'Internal Quality Assurance' Server is only accessible to the following staff:

Position	Requirement	Reason
Workplace Assessors	Access to the 'Assessor Tracking' spreadsheet, workplace Reviews and IQA paperwork	To complete workplace reviews, cause for concerns, disciplinary documents and IQA paperwork
Internal Quality Assurers	Access to IQA paperwork	Completion of IQA paperwork
Chief Operating Officer	Access to the 'Assessor Tracking' spreadsheet and Workplace Reviews.	To gain current and historical information on Apprentices progress and IQA documents for Quality review purposes
Centre Compliance Manager	Access to the 'Assessor Tracking' spreadsheet, workplace reviews and IQA paperwork.	To gain current and historical information on Apprentices progress and IQA documents for Quality review purposes
Apprenticeship Services Manager	Access to the 'Assessor Tracking' spreadsheet and Workplace Reviews.	To gain current and historical information on Apprentices progress
Work-Based Learning Manager	Access to the 'Assessor Tracking' spreadsheet, workplace reviews and IQA paperwork.	To gain current and historical information on Apprentices progress and IQA documents for Quality review purposes

3. The 'Apprenticeships' Server is only accessible to the following staff:

Position	Requirement	Reason
Chief Operating Officer	Overarching access as a company director	Overarching access as a company director
Centre Compliance Manager	Access to documents	Access to documents for Quality review purposes
Apprenticeship Services Manager	Access to documents	Access to documents for Learner DATA review and to gain DATA on learners to upload in to PICS MIS
Finance Manager	Access to documents	Uploading documents and entering DATA in to them on the system
Pastoral Support	Access to documents	Uploading documents and entering DATA in to them on the system
Business Development Manager	Access to documents	Uploading documents to the system
Chief Executive Officer	Overarching access as a company director	Overarching access as a company director

DATA Unable to be Erased

1. Learners on Apprenticeships

DATA	Main Reason	Supplementary Notes
Name, Date of Birth and Ethnicity	Held via an awarding body for registration and certification purposes	Held on SETA's MIS for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
Medical and Learning Difficulty Declaration	Used to assist learning	Held on SETA's MIS for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
Address	Used for correspondence and sending out certificates	Held on SETA's MIS for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
Prior Certification/Certification received whilst at SETA	Used for evidencing parts of Apprenticeship Standards and Frameworks on completion	Held on SETA's MIS for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
SETA enrolment form	Proof of Apprenticeship	Held on SETA's Secured Server
Agreement on acceptable behaviour form	Used to assist learning	Held on SETA's Secured Server
ACE declaration	Must be held for 3 years after completion for proof of authorization	Stored via ACE organisation and on SETA's Secured Server
Student photo/video consent form	Explicit consent held for publishing/displaying photos and videos of Awards gained and for SETA's hall of fame during and after apprenticeship has ended	Held on SETA's Secured Server
contract of employment	Mandatory form as proof of Apprenticeship contract	Held on SETA's Secured Server
job description and training requirements form	A Mandatory form held throughout Apprenticeship	Held on SETA's Secured Server
Internal Quality Assurance documents	Mandatory forms required for Certification via Awarding bodies	Held on SETA's Secured Server
learner workplace reviews	Mandatory forms required for Apprenticeship progress and Ofsted	Held on SETA's Secured Server
learner cause for concerns	Used to assist learning	Held on SETA's Secured Server
learner disciplinaries	Used to assist learning	Held on SETA's Secured Server
College Service Level Agreement	Mandatory form as proof of Qualifications studied outside of SETA	Held on SETA's Secured Server
SETA commitment statement form	Mandatory agreement between Learner, Employer and SETA.	Held on SETA's Secured Server

DATA Unable to be Erased

2. Learners who have completed an Apprenticeship and left SETA

DATA	Main Reason	Supplementary Notes
Name, Date of Birth and Ethnicity	Held via an awarding body for Certification purposes	Cannot be removed by SETA
	Held by SETA on various forms	Held on SETA's MIS for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
Medical and Learning Difficulty Declaration	Used to assist learning and proof of extra time allowances during examinations	Held on SETA's MIS for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
Address	Held by SETA on various forms	Held on SETA's MIS for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
Prior Certification/Certification received whilst at SETA	Used for evidencing parts of Apprenticeship Standards and Frameworks on completion	Held on SETA's MIS for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
SETA enrolment form	Proof of Apprenticeship	Held on SETA's Secured Server for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
ACE declaration	Must be held for 3 years after completion for proof of authorization	Stored via ACE organisation and on SETA's Secured Server
Contract of employment	Mandatory form as proof of Apprenticeship contract	Held on SETA's Secured Server for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
Job description and training requirements form	A Mandatory form held throughout Apprenticeship	Held on SETA's Secured Server for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
Assessment and Internal Quality Assurance documents	Mandatory forms required for Certification via Awarding bodies	Held on SETA's Secured Server and cannot be erased until 3 years from date of Certification in line with Awarding Body requirements.
learner workplace reviews	Mandatory forms required for Apprenticeship progress and Ofsted	Held on SETA's Secured Server for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
learner cause for concerns	Used to assist learning	Held on SETA's Secured Server for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
learner disciplinaries	Used to assist learning	Held on SETA's Secured Server for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
College Service Level Agreement	Mandatory form as proof of Qualifications studied outside of SETA	Held on SETA's Secured Server for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.
SETA commitment statement form	Mandatory agreement between Learner, Employer and SETA.	Held on SETA's Secured Server for funding purposes. Started/completed Apprentices between 2007 and 2013 cannot be deleted until 01/01/2023. Starts

		Started/completed Apprentices between 2014 and 2020 cannot be deleted until 01/01/2031.

3. SETA Staff

DATA	Main Reason	Supplementary Notes
Name, Date of Birth and Ethnicity	Required for identification and staff records	Held in paper-based format in locked HR files at SETA. Also held on Awarding Body secured electronic systems.
Medical and Learning Difficulty Declaration	Required for identification of support requirements and staff records, and proof of extra time allowances during examinations	Held in paper-based format in locked HR files at SETA.
Address	Proof of residence and eligibility to work in the UK	Held in paper-based format in locked HR files at SETA.
Prior Certification/Certification received whilst at SETA	Proof of qualifications for job role, required by Awarding bodies and staff records	Held in paper-based format in locked HR files at SETA. Also held on Awarding Body secured electronic systems.
Contract of employment	Mandatory requirement for explanation of job description and duties	Held in paper-based format in locked HR files at SETA.
Internal Quality Assurance documents	Mandatory requirement for Certification from Awarding Bodies	Held on SETA's Secured Server and cannot be erased until 3 years from date of Certification in line with Awarding Body requirements.
Application for Employment form	Required for suitability for job position and audit purposes	Held in paper-based format in locked HR files at SETA.
CV	Proof of qualifications for job role, required by Awarding bodies and staff records	Held in paper-based format in locked HR files at SETA. Also held on Awarding Body secured electronic systems.
DBS Check form	Mandatory requirement	Held in paper-based format in locked HR files at SETA.
Bank Authorisation form	Required for PAYE	Held in paper-based format in locked HR files at SETA.
Appraisals	Required for staff development	Held in paper-based format in locked HR files at SETA.

4. Commercial Learners

DATA	Main Reason	Supplementary Notes
Name, Date of Birth and Ethnicity	Held via an awarding body for Certification purposes	Cannot be removed by SETA
	Held by SETA on various forms	Can be removed only after course has been completed
Medical and Learning Difficulty Declaration	Used to assist learning and for proof of extra time during examinations.	Can be removed only after course has been completed
Address	Proof of residence and eligibility to work in the UK	Can be removed only after course has been completed
Prior Certification	Evidencing entry requirements on qualifications	Can be removed only after course has been completed
Application form	Held by SETA as proof of enrolment	Can be removed only after course has been completed

Assessment and Internal Quality Assurance documents	Mandatory forms required for Certification via Awarding bodies	Held on SETA's Secured Server and cannot be erased until 3 years from date of Certification in line with Awarding Body requirements.

5. Subcontractors

DATA	Main Reason	Supplementary Notes
Contracting College name, address, main contact name, e-mail address and signature	Must be kept for contractual reasons	Can be removed only after contract has ended
Learner name	Must be kept for contractual reasons	Can be removed only after contract has ended

6. Employers

DATA	Main Reason	Supplementary Notes
Policy Number, Name of policy holder, Date of commencement and Date of expiry	Proof of Employers' Public Liability Insurance	Can be removed only after Apprentice has completed and no other Apprentice for the company is live.
Policy Number, Name of policy holder, Date of commencement and Date of expiry	Proof of Employers' Liability Insurance	Can be removed only after Apprentice has completed and no other Apprentice for the company is live.
Employer Name, Employer Signature and representative Name	SETA commitment statement form held as proof of Apprenticeship delivery	Can be removed only after Apprentice has completed and no other Apprentice for the company is live.
Employer Name, Address, Telephone Number, Contact Name and Mentor name	Mandatory Individual Learner Plan for Apprentice	Can be removed only after Apprentice has completed and no other Apprentice for the company is live.
Employer Name, Address, Website, Line Manager, Line manager Contact Details and Job Information	Held on job description and training requirements form which forms part of the Apprenticeship Contract	Can be removed only after Apprentice has completed and no other Apprentice for the company is live.

Subject DATA Portability Request

1. DATA Subject Details										
Title *(Please Tick)*	Mr		Mrs		Miss		Ms		Other	
First Name(s)				Surname						
Date of Birth		Email Address								
Current Address	House No.									
	First Line									
	Second Line									
	Third Line									
	City									
	Postcode									
Home Tel No.										
Work Tel No.										
Mobile Tel No.										
FAX Tel No.										

2. Details of identification provided to confirm identity of DATA subject

Subject DATA Portability Request

3. Details of Third Party Acting on Behalf of DATA Subject *(if applicable)*										
Are you acting on behalf of the data subject with their written or other legal authority?							YES		NO	
If 'Yes' please state your relationship with the data subject *(e.g. parent, legal guardian or solicitor)*										
Please enclose proof that you are legally authorised to obtain this information and complete the information require below *(e.g. a letter of authority, letters or official forms addressed to you on behalf of the data subject or power of attorney)*										
Title *(Please Tick)*	Mr		Mrs		Miss		Ms		Other	
First Name(s)					Surname					
Email Address										
Current Address	House No.									
	First Line									
	Second Line									
	Third Line									
	City									
	Postcode									
Home Tel No.										
Work Tel No.										
Mobile Tel No.										

5. Declaration	
DATA Subject Declaration	**Third Party Declaration** *(if applicable)*
I, ……, the undersigned and person identified in (1) above, hereby request that SETA provide me with the all held documents and data about me in portable format and I take full responsibility of that which is provided.	I, ……, the undersigned and person identified in (4), hereby request that SETA provide me with the all held documents and data on the data subject identified in (1) in portable format and I take full responsibility of that which is provided.
Signature: Date:	Signature: Date:

DATA Protection Impact Assessment

Subject:		**Ref.**	SDPIA-000
Assessment Carried out by:			
Date of Assessment:		**Review Date:**	

1. Need for a DPIA Identification
Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

2. Description of the Processing
Nature of the Processing *Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?*
Scope of the processing *Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?*
Context and purpose of the processing what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in?

DATA Protection Impact Assessment

Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
3. Consultation Process
Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

4. Necessity and Proportionality Assessment
Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

5. Risks Identification and Assessment			
Describe source of risk and nature of potential impact on individuals. *To include associated compliance and corporate risks as necessary.*	**Likelihood of harm** *(Remote, possible or probable)*	**Severity of harm** *(Minimal, significant or severe)*	**Overall risk** *(Low, medium or high)*
6. Identify measures to reduce risk			

DATA Protection Impact Assessment

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** *(Eliminated reduced accepted)*	**Residual risk** *(Low, medium or high)*	**Measure approved** *(YES or NO)*

DATA Protection Impact Assessment

7. Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:	DPO advice accepted or overruled by:	DPO advice accepted or overruled by:
Comments:		
Consultation responses reviewed by:	Consultation responses reviewed by:	Consultation responses reviewed by:
Comments:		
This DPIA will kept under review by:		
Summary of DPO advice:	Summary of DPO advice:	Summary of DPO advice:

DATA Protection Impact Assessment Register

The following table provides information on areas SETA has carried DATA Protection Impact Assessments.

Ref.	Subject	Assessment Carried out by	Date of Assessment	Review Date	Risk outcome
SDPIA-001	Biometric Hand Scanner	Peter Hurlstone	29/05/2018	30/05/2019	Low
SDPIA-002	Voice DATA Capture	Peter Hurlstone	11/06/2018	12/06/2019	Low
SDPIA-003	Biometric Temperature Recording	Peter Hurlstone	10/12/2020	11/12/2021	Low

All DATA Protection Impact Assessments are located in **Annex N**.