


GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

(SBMAK LIMITED –Trading as “STEP UP EDUCATION CENTRE”)

	Policy & Procedure Support Services Manual	
Subject:	General Data Protection Regulation (GDPR) Policy	
Procedure No.: 9A	Date of Publication	Date: 21 April 2025
Issue No.:	1	Date: 21 April 2025
Location:	Policy Manual	
Date of next review:	21 April 2025	
Approved by:	The Quality Assurance Manager	

1. INTRODUCTION

1.1. This document outlines our legal requirements under the General Data Protection Regulations and the processes for how Step up (SBMK Limited) meets them.

1.2. SBMK Limited –Trading as Step Up Education Centre: Is committed to ensuring your privacy is protected in accordance with Data Protection Standards.

1.2.1. The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU) It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

1.2.2. The Regulations cover both written and computerised information and the individual's right to see such records.

1.2.3. It is important to note that the Regulations also cover records relating to service users, visitors, staff and volunteers.

1.2.4. The Internal Quality Assurance Manager has overall responsibility for data protection within Step up but each individual processing data is acting on the controller's behalf and therefore has a legal obligation to adhere to the Regulations.

2. PRIVACY POLICY

2.1.1. In this privacy policy we will set out how we collect and process personal data from employees, Care provider employers and learners and awarding organisations. We will also set out our data breach procedures.

2.2. Employee – Tutor Assessor/ Internal Quality Assurance

2.2.1. In the collection of this data, we will ask our employees for their explicit consent for personal data to be collected and used. This consent will form the lawful basis for the processing and will be asked for at the time of employment.

2.2.2. A clear information will be provided to enable the employee to take an informed decision. Such information will include:

- Information we collect
- How we store this data
- What rights employees have to access their data
- The right for employee data to be deleted on request
- The reasons why we are storing employee data
- How long we keep this data
- Who we share this data with

2.3. INFORMATION WE COLLECT FROM EMPLOYEE

2.3.1. We collect information for the purposes of employment in any of Step up premises. The information we need for this are:

2.3.1.1. Name and address, current CV, all qualifications for the role applied for, contact information to include telephone numbers and email address.

2.3.1.2. References from past employers, bank account details, National Insurance number, photographic ID, work permit (if applicable) and DBS details if issued with one.

2.4. How we store this data?

2.4.1. All data collected will be stored digitally on secure computers and paper files will be stored in locked cabinets.

2.4.2. Limited data such as name, address, e-mail, telephone number and next of kin contact details will be stored on the works mobile phone.

2.5. What rights employees have to access their data?

2.5.1. Employee information is held in a transparent and lawful manner and can be accessed on request at any time in writing.

2.6. The right for employee data to be deleted on request

2.6.1. An employee has the right of erasure of all personal data held when they cease to work for the Step up with the exception of information we are lawfully obliged to keep for Government agencies.

2.7. The reasons why we are storing employee data.

2.7.1. The reason we hold personal data on our employees is to enable us operate a lawfully and effective education and training provision.

2.7.2. We have an obligation to our awarding organisations to provide employee with the correct qualifications and experience to carry out the duties required. Also because we deal with vulnerable service users – males and females, we are legally obliged to ensure that you have an up to date Disclosure Barring Service Check (DBS).

2.8. How long we keep this data?

2.8.1. We will keep this data for 5 (five) years from the day the employee leaves the organisation. We have to keep all payroll data for a period of 5 years from the last date the employee worked.

2.9. Who we share this data with?

2.9.1. By consenting to using your personal data for the purposes of employment, we will share your information with third parties for the purposes of quality and compliance audit only. This information will never include information such as bank account

details but will include information to show your suitability for the role. We will only give full information if requested to do so by Law Enforcement Agencies.

3. INFORMATION WE COLLECT FROM OUR LEARNERS

3.1. To ensure that we can process your application for learning and development services with us, we will be processing the following information:

- Your full name, address and contact details and next of kin information.
- Any specific medical conditions that may affect your ability to carry out practical tasks such as moving and handling, CPR etc.
- Any specific learning needs that you may be required to disclose, as it will enable us to plan any possible adjustment to accommodate your needs.
- Details relating to the methods through which your training is being funded. If you are funding your training, then we will take payment through cash, standing order or direct debit. If your training is being funded by your employer or other funding agencies, then we will deal with the organisation funding this, or any other party that you have nominated or has agreed to pay for your training.

3.2. Are we likely to need sensitive Personal data?

3.2.1. Yes. In order to ensure that we can provide the necessary learning and development to you as an individual, and to enable your registration with awarding body, your date of birth and gender will be necessary. You must also provide a photo identity card, preferably a copy of your passport.

3.3. Why we need the information?

3.3.1. We need this information to:

- 3.3.1.1.** Fulfil our contract with you. Providing your training services at the start of your time with us as well as adapting those services as your training needs change.
- 3.3.1.2.** In medical situations. To ensure that we have the necessary medical information about you to be able to pass onto medical professionals in the event of emergencies. This will also help your assessor to plan your assessment better. To comply with the awarding organisation requirements, law and funding agent requirement.

3.4. CCTV –CLOSED-CIRCUIT TELEVISION

3.4.1. Step Up Education Centre uses CCTV systems to maintain the security of the premises, ensure the safety of staff, learners, visitors, and to protect property.

3.5. Purpose of CCTV Use:

- Prevention and detection of crime
- Ensuring the safety and security of staff, learners, visitors, and property
- Assisting with internal investigations.

3.6. Location of Cameras:

- CCTV cameras are placed in prominent locations around the premises, clearly visible and with appropriate signage.
- Cameras are not positioned in private areas such as toilets or changing rooms.

3.7. Data Storage and Security:

- CCTV footage is stored securely on encrypted digital storage devices.
- Access to footage is strictly controlled, limited to authorised personnel only, typically the Internal Quality Assurance Manager or nominated senior staff.

3.8. Retention Period:

- CCTV footage will be retained for 30 days, after which it will be automatically deleted unless needed for ongoing investigations.

3.9. Access and Disclosure:

- Individuals recorded on CCTV have the right to request access to footage under GDPR regulations. Requests must be made in writing to the Internal Quality Assurance Manager.
- CCTV footage may be shared with law enforcement agencies where required by law or to assist in criminal investigations.

3.10. Individual Rights:

- Individuals have the right to request footage deletion if no longer necessary for the purposes outlined above.
- Requests must be evaluated against legitimate interests, legal obligations, and rights of other individuals.

3.11. Transparency and Notification:

- 3.11.1.** Signage will be prominently displayed notifying individuals of CCTV operation, stating the purpose, and identifying the data controller.

3.12. How do we store your data?

- 3.12.1.** All data collected will be stored digitally on secure computers and paper files will be stored in locked cabinets.
- 3.12.2.** Limited data such as name, address, e-mail, telephone number and next of kin contact details will be stored on the works mobile phone.

3.13. What rights an individual have to access their data?

- 3.13.1.** Your information is held in a transparent and lawful manner and can be accessed on request at any time in writing.

3.14. The right for Learner data to be deleted on request

- 3.14.1.** You have the right of erasure of all personal data held when you cease to receive service from the Step Up Education Centre with the exception of information we are lawfully obliged to keep for awarding organisation and Government agencies.

3.15. How do I withdraw consent or change my preference?

- 3.15.1.** You can object to us processing your data at any time by:
- Informing the centre manager
 - By contacting us and letting us know what you would like to change

3.16. Be aware that in some cases, objecting to the processing or sharing of your information may result in a service being withdrawn or us being unable to comply with the law or our contract with you. You will be informed of how we can or cannot comply with your request, when /if you were to make such a request.

3.17. The reasons why we are storing learner/ client data.

3.17.1. The reason we hold personal data on our learner or client is to enable us operate a lawfully and compliance with the awarding organisation requirements.

3.18. How long we keep this data?

3.18.1. We will keep this data for 5 (five) years from the day the service user/ client leaves the organisation. Due to the nature of the services we provide and our requirements to adhere to the government retention guidelines, these may change from time to time. If you do not wish us to retain your data, then you have the right to be forgotten.

3.18.2. At your request, we will destroy your data where we can legally do so and / or where we do not have a legitimate interest to retain such information e.g. any accidents that you may have had during your time with us. If your data is required for statistical analysis, then your personal data will be anonymised to ensure that it is no longer personally identifiable.

3.19. Who we share this data with?

3.19.1. By consenting to using your personal data for the purposes of provision of education and training services, we will share your information with third parties. We will only give full information if requested to do so by Law Enforcement Agencies.

3.19.2. We may share your data with the following third-parties:

- Medical professionals e.g. ambulance service, general practitioner, locum, hospital, mental health team if emergencies arise.
- Awarding Organisation e.g. City and Guilds, TQUK, AOFAQ to enable your registration and certification.
- Funding services e.g. skills for care and any other relevant funding agencies contributing to your learning and development.
- Police – in the event of any matters involving the law.
- Industry compliance / audit – where we are required to comply with industry requirements e.g. accreditations, auditors etc. we may need to share only data

that is limited to fulfilling that purpose necessary to demonstrate compliance. This may therefore fall under the category of legitimate interest or legal obligation, depending on the nature of the audit/compliance requirement.

- Government services – Learning register services, Ofqual etc. – as required by law or order.

3.20. We use consistent third-parties who act as data processors on our behalf to provide specific services. We may share your data with them to enable us to undertake the activities as set out above. They themselves may then become data controllers once your data is shared with them. They may also introduce you to us or us to you e.g. city and guilds learners' location services to signpost their approved centre etc.

3.21. All the companies above either comply with our privacy policy or have appropriate security measures in place in order that they comply with the requirements under data protection and GDPR legislation.

3.22. From time to time, we may seek your consent to share information with other third-parties not included in the list above. In this instance, we will seek your explicit consent and detail what information will be shared.

3.23. What safeguards are in place to protect my personal data?

3.23.1. Step Up Education Centre operates a Security by design and by default methodology that means we are continually checking the security, both new and current. This enables us to adhere to the Privacy by Default and By Design principles.

3.23.2. We will not change the use of your personal data in respect of this policy or share your data with a third party (other than those outlined above), without informing you or obtaining your consent where possible unless it is for our legitimate interest and your interests, rights and freedoms are not affected.

4. SECURITY

4.1.1. Step Up Education Centre operates a Privacy by Design and By Default policy. This means that before we use your data we have already considered the potential impact on you were your data to be lost, stolen, shared or compromised.

4.1.2. We undertake routine reviews of our processes and security policies to ensure that we can take all reasonable precautions in protecting your data.

4.1.3. Where at all possible we encrypt all information that is either stored or transmitted to third parties. Where data is stored or transmitted to a Third Country (any country outside of the European Economic Area (EEA)) we will ensure appropriate adequacy protection is in place in accordance with Data Protection Legislation.

4.1.4. Consequently, we may also need to sometimes undertake further security and screening questions when undertaking our routine dealings with you these are there to protect your personal data and security. Whilst we undertake all reasonable precautions, encryption, software updates and patches, we cannot guarantee the safety of data transmitted over the internet.

5. SUMMARY OF PROCEDURE

5.1. When an employee or learner account is set up by Step Up Education Centre the following procedures are put in place.

5.2. We store the account documents in a locked cabinet.

5.3. The account invoice details are stored on the computer.

5.4. A tracking record is created and stored in a locked cabinet.

5.5. Contact details are entered on to a database and used to contact you by telephone, e-mail and post.

5.6. The relevant contact details are also stored onto a password protected mobile phone.

5.7. Relevant Contact details are accessible to Assessor / Tutor/ IQA that are delegated to arrange your training, carry out an initial assessment and plan your review and progress until you achieve your qualification etc.

5.8. All computer digital records are protected with several layers of software to protect from cyber-attacks and virus attacks.

5.9. All digital records are password protected.

6. DATA BREACH PROCEDURES

6.1. Power of the Information Commissioner

6.2. The following are criminal offences, which could give rise to a fine and / or prison sentence:

- The unlawful obtaining of personal data
- The unlawful selling of personal data
- The unlawful disclosure of personal data to unauthorised persons

6.3. INFORMING THE INFORMATION COMMISSIONER'S OFFICE

6.3.1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification is not made to the ICO within 72 hours, it shall be accompanied by reasons for the delay.

6.3.2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

6.3.3. Also you have the right to make a complaint at any time to the Information Commissioner's office (ICO), the UK supervisory authority for data protection issues. You can contact the Information Commissioner Office on 0303 123 1113 or via e-mail on <https://ico.org.uk/global/contact-us/email/>

Or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

If you have any questions about this privacy notice, please contact the Registered Manager sbmak@stepupedu.com