Data protection policy

Purpose

The organisation is committed to being transparent about how it collects and uses the personal data of its workforce, volunteers, and customers, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, volunteers and former employees, learners, project participants, external suppliers and customers.

The organisation has appointed Will Sanderson as Data Protection Champion. He can be contacted by writing to the company's main address in Folkestone.

Definitions

"Personal data" is any information that relates to a natural person who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

The organisation processes personal data in accordance with the following data protection principles:

- The organisation processes personal data lawfully, fairly and in a transparent manner.
- The organisation collects personal data only for specified, explicit and legitimate purposes.
- The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The organisation keeps personal data only for the period necessary for processing.
- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The organisation tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where the organisation processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

The organisation will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered is held in the individual's personnel, learner and customer files (in hard copy or electronic format, or both), and on HR systems. The organisation keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Social Enterprise Kent defines personal data as data which relates to an identified or identifiable natural person. This is based on Article 4 of the GDPR. This does not relate to businesses or companies which are not “natural persons”. Generic business email addresses (eg “info@companya.co.uk”) are therefore not covered by GDPR.

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA)
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;

The organisation will also provide the individual with a copy of the personal data undergoing processing.

To make a subject access request, the individual should send the request to the company’s main office address. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify his/her identity and the documents it requires.

The organisation will normally respond to a request within a period of one month (30 days) from the date it is received.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an

individual submits a request that is unfounded or excessive, the organisation will notify him/her that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

Data security

The organisation takes the security of personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Individual responsibilities

Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, or apprenticeship. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;

- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

TRAINING

The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

EQUALITY DATA COLLECTION AND MONITORING

Although there is no legal duty to collect monitoring information against individual protected characteristics, in order to demonstrate due regard to the aims of the general equality duty held by public bodies, Social Enterprise Kent will sometimes collect equality data upon which to measure its equality and diversity profile.

Equality monitoring relates to one or more of the nine protected characteristics established by the 2010 Equality Act: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation and if monitored properly, particularly in relation to recruitment, can help the organisation to better balance its workforce and develop fair opportunities for all. Equality monitoring for staff and volunteers will also assist Social Enterprise Kent to identify and address any inequalities in the application of employment and placement practices.

Social Enterprise Kent will keep all collected equality data pertaining to individuals confidential and securely stored whilst awaiting periodic analysis in line with the above aims, after which it will be destroyed.

STORAGE OF RECORDS

The Company stores most of its records on-line, on Company servers which are located within the EU and protected by firewalls and virus software. Permission levels for Company employees to access specific files and folders within the server (and other software used by the Company, such as PICS, Salesforce) is managed by the Company's IT Manager, delegated by the SEK Board. Any unusual requests for access will require authorisation by a Company Director.

The Company also maintains a contract with a 3rd party IT firm, who provide backup support for the Company's servers in the event of an emergency.

Records held electronically are backed up electronically overnight.

Certain Company records are still required to be stored in paper format (mainly those for ESF-funded projects). These records are stored off-site in a bespoke storage facility managed by a 3rd party storage company. These records are securely destroyed after the retention period has expired.

COVID 19 Track and Trace

For the purpose of contact tracing, all that is required is the persons name and contact details. We must tell people why we are collecting information and how this will be used. Transparency is important and is required by data protection law. The information gathered must not be viewed or photographed by others.

The COVID 19 incubation period is 14 days, some additional time should be allowed to allow for the track and trace process to operate, but overall retention should be short and not exceed 21 days. This data should not be held any longer than necessary and it has been collated for a specific purpose. Deletion of data must be undertaken securely. When collecting for the purpose of contact tracing, the data must not be added to any marketing database.

Company's Main Office Address

Social Enterprise Kent

The Marigold Centre, 65 Shaftesbury Avenue

Cheriton, Kent

CT19 4NS

Last reviewed: July 2021
Next review date: July 2024

Signed:

Claudia Sykes (Chief Executive Officer)

Data being processed	Reason	Reason – detail	Retention period
Recruitment data for staff (CV, references, application form, interview records)	Legitimate interests	Employees and future employers, funders and regulators would expect this data to be processed and retained	Duration of employment and then 3 years from end of employment
Information required for DBS check (eg copies of passport)	Legal requirement	Required for certain employees working with vulnerable adults	Copies of documents to be deleted after processing (ie after the DBS check has been done). DBS number and numbers of documents checked will be logged as evidence of compliance with Right to Work/Safeguarding
Copy of car insurance annually (if employee drives for work)	Contract	Required as part of employment contract to evidence staff safe to drive	To delete after checking
Payroll data (NI number, bank details, home address)	Contract	Information required for processing of employee pay	Duration of employment, and then deleted 6 months after employee leaves
Employment records (supervisions, appraisals, notes of meetings, sickness absence, training certificates)	Legitimate interests	Required to evidence performance of job role as set out in employment contract and job description, employee would expect this to be processed and retained	6 years
Wage records, payslips, expense claims,	Legal requirement	Required for compliance with Minimum Wages Act	3 years
Record of PAYE and NI paid, evidence of SSP,	Legal requirement	Taxes Management Act	6 years

SMP, redundancy payments			
Accounting records (including all records relating to sales and purchases, eg customer invoices, sessional invoices and backup sheets etc)	Legal	Required for compliance with the Companies Act	Must be retained for 6 years after current accounting period
Individual records for ESFA-funded training and BBO (eg name, NI number, address, evidence of right to stay/work in EU; any medical information required to enable access to training and support)	Contract	Required for government contracts (SFA) and ESF - Big Lottery Fund	ESF funded, must be retained 6 years after end of project
Photos of people taken for marketing purposes (eg for website, at events, for leaflets)	Consent	Used for publicity and marketing purposes	To delete 3 years after project ends, or event happened
Personal information on Ageless Thanet participants and all SEK volunteers (name, Email, address), and health restrictions	Legitimate reason	Required to enable project staff to contact participants and volunteers, and make any reasonable adjustments to allow people to participate	Will be destroyed after participant has taken part in project, or after project ends (2020) whichever is earlier
Information from past government-funded projects (eg ECCE)	Contract	Required to be kept for evidence of project, as set out in Ecorys contract	6 years after end of project
Learner records for any individuals on non-accredited day training (eg where people have booked themselves). course attendance sheets with names, emails	Consent	Required in case of any queries on the course, and for quality assurance processes	6 months after individual attended the course
Learner records on accredited day training (eg IOSH)	Legal	Required as part of evidence for	Will be destroyed after awarding

		awarding body accreditation	body inspection (usually 1-2 years)
Information (Email addresses, phone numbers, business address) on existing customers	Legitimate reason	Required as part of business activity; expected to be held on file by existing customers	Will be deleted on request from customer, other than where required as part of compliance for Companies Act (retention of company accounting records, including invoices)
Information (Email addresses, phone numbers, business address) on existing suppliers	Legitimate reason	Required as part of business activity; expected to be held on file by suppliers	Will be deleted on request from supplier (other than as required as compliance for Companies Act as noted above)
Contact and professional information on subcontractors and sessional trainers	Legitimate reason	Required as evidence that subcontractors and sessionals are competent to deliver training	Will be deleted 6 years after training delivered
Information on new customers used for marketing purposes (Email addresses, phone numbers, business addresses)	Consent		Will be deleted on customer request