Data Protection Policy

Supplytrain CIC is registered with the Information Commissioner's Office

Purpose of policy

The purpose of this policy is to enable Supplytrain to:

- Comply with the law in respect of the Data Protection Act 2018 ("the Act") and General Data Protection Regulations regarding the data it holds about individuals;
- Follow good practice;
- Protect Supplytrain customers, staff, participants in work schemes and other individuals;
- Protect the organisation and individuals from the consequences of a breach of its responsibilities;
- Maintain the confidentiality of business information where appropriate

General Policy Statement

Supplytrain will:

- Comply with both the law and good practice
- Respect individuals' rights
- Be open and honest with individuals whose data is held
- Provide training and support for staff and contractors who handle personal data, so that they can act confidently and consistently.

Supplytrain recognises that its first priority under the Act and General Data Protection Regulations is to avoid causing harm to individuals. In the main this means:

- Keeping information securely in the right hands
- Holding good quality information.

Secondly, the Act and the General Data Protection Regulations aim to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. To do this, Supplytrain will be:

- Open and transparent
- Will allow individuals choice over how data is held and how it is used
- Will allow individuals access to the data that is held about them.

Scope of this policy - Personal data and confidentiality

This policy applies to information relating to identifiable individuals (Data Subjects), even where it is technically outside the scope of the Data Protection Act or the General Data Protection Regulations, by virtue of not meeting the strict definition of 'data' in the Act. Reference is also made in this document to Confidentiality. Confidentiality applies to a wider range of information

than personal data including information about the company, other organisations that the company deals with and information that is not held electronically.

Responsibilities

Directors

The Board of Directors recognises its overall responsibility for ensuring that Supplytrain complies with its legal obligations.

Data Protection Officer

The Data Protection Officer is currently the Finance Manager with the following responsibilities:

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors

Staff & Contractors

All staff and contractors are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. Staff and contractors are required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities. (See Appendix B.)

Enforcement

Significant breaches of this policy will be handled under Supplytrain's disciplinary procedures.

Data Protection and Supplytrain's Business Model

Supplytrain works with small businesses and young people promoting apprenticeships and other work related activity such as traineeships, employability training the government's Kickstart scheme. In some circumstances we will collect information on behalf of another organisation.

Categories of Data Subjects

Businesses – that get in touch with Supplytrain via the telephone, email or web-sites

Staff – Employees and Contractors that work with us on our programmes

Work scheme participants – taking part in one of the work related schemes we promote

Other businesses – that we have a business relationship with

Key risks

Supplytrain has identified the following potential key risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately)
- Insufficient clarity about the range of uses that data will be subject to
- Failure to offer choice about data use when appropriate
- Breach of security by allowing unauthorised access
- Harm to individuals if personal data is not up to date
- Insufficient clarity about the way personal data is being used
- Failure to offer choices about use of contact details
- Data Processor contracts with other organisations
- Misuse of personal information by staff or contractors
- Poor web site security
- The giving away of information through "social engineering" - staff may be tricked into giving away information, either about participants or colleagues, especially over the phone.

Procedures to mitigate the potential risks

Setting security levels

Access to information on the main computer system will be controlled by function and secure passwords.

Accuracy

Supplytrain will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held in as few places as necessary, and all staff and contractors will be discouraged from establishing unnecessary additional data sets.
- Effective procedures will be in place so that all relevant systems are updated when information about any individual changes.
- Staff or contractors who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.

Retention periods

Supplytrain will establish retention periods for the following categories of data:

- Staff
- Contractors
- Businesses

- Work scheme participants

Commitment to Data Subjects

Supplytrain is committed to ensuring that in principle Data Subjects are aware that their data is being processed and

- for what purpose it is being processed;
- what types of disclosure are likely; and
- how to exercise their rights in relation to the data.

Data Subjects will generally be informed of this commitment and their rights in the following ways:

- Staff: in the Staff Information folder
- Contractors: in the Contractors Information folder
- Businesses: via website Privacy Statement (Appendix A) and the Employers Information folder
- Work scheme participants (Apprentices/Kickstart): in the Participants Information folder

Standard statements will be provided to staff for use on forms where data is collected.

Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

Subject Access Requests

- **Responsibility** Any subject access requests will be handled by the Data Protection Officer.
- **Procedure for making request** Subject access requests must be in writing. All staff and contractors are required to pass on anything which might be a subject access request to the Data Protection Officer without delay.
- **Provision for verifying identity** Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information.
- **Procedure for granting access** The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

Consent from staff

Consent will normally not be sought for most processing of information about **staff** and **contractors**, with the following exceptions:

- Staff and contractor details will only be disclosed for purposes unrelated to their work for Supplytrain (e.g. financial references) with their consent.

Marketing Activity

Supplytrain will treat the following unsolicited direct communication with individuals as marketing:

- Promoting any Supplytrain services;
- Marketing the products of Supplytrain including those branded by other names;
- Seeking donations and other financial support;
- Promoting sponsored events and other fundraising exercises;
- Marketing on behalf of any other external company or voluntary organisation;
- Provision of information relevant to promoting the aims of the company

Opting out

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given a clear opt out. If it is not possible to give a range of options, any opt-out which is exercised will apply to all Supplytrain marketing.

Staff/contractor training and acceptance of responsibilities

- **Documentation** Information for staff and contractors is contained in the staff folder.
- **Induction** All staff who have access to any kind of personal data will have their responsibilities outlined during their induction procedures and will be asked to sign a Confidentiality statement.
- **Continuing training** Supplytrain will provide opportunities for staff to explore Data Protection issues through training, team meetings, and supervisions.

Data Processor Contracts

When work is outsourced, which involves the contracting organisation in having access to personal data, there will be a suitable written contract in place, paying particular attention to security. When Supplytrain acts as a Data Processor for another organisation we ensure there is a suitable written contract in place.

Reporting of personal data breaches

A personal data breach is the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A personal data breach may be from an accidental or a deliberate cause. It could include, but is not limited to:

- Access by an unauthorised third party, e.g. via hacking or other forms of unauthorised access to our network, email account/s or devices;
- Sending personal data to the wrong recipient/s, e.g. through incorrectly addressed emails or bulk emails that reveal all recipients' email addresses;
- The loss or theft of devices, including laptops or USB drives;
- The alteration or destruction of personal data without permission.

Staff are trained to recognise personal data breaches. On becoming aware of a breach, staff will immediately report it to the Management Team who will assess the breach for potential consequences for individuals.

If the personal data breach is likely to result in a risk to the rights and freedoms of individuals, the DPO will make a report to the Information Commissioner's Office ("ICO") within 72 hours.

If the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will inform the individuals themselves without undue delay, and within 72 hours.

The DPO will record all breaches of personal data, whether or not they have been reported to the ICO. The record will include:

- The facts of the personal data breach
- Its effects
- The remedial action taken

The Management Team will investigate whether the breach was a result of human error or a systemic issue, and will establish and put in place processes to safeguard against a recurrence.

Last reviewed 05/10/2021

F Lauer Deaves

Appendix A: Privacy Statement

When you request information from Supplytrain, sign up to our newsletter or register an interest in the Kickstart scheme, Supplytrain obtains information about you. This statement explains how we look after that information and what we do with it.

We have a legal duty under the Data Protection Act to prevent your information falling into the wrong hands. We must also ensure that the data we hold is accurate, adequate, relevant and not excessive.

Normally the only information we hold comes directly from you. Whenever we collect information from you, we will make it clear which information is required in order to provide you with the information, service or goods you need. You do not have to provide us with any additional information unless you choose to. We store your information securely on our computer system, we restrict access to those who have a need to know, and we train our staff in handling the information securely.

We may like to contact you in future to tell you about other services we provide, and ways in which you might like to support Supplytrain. You have the right to ask us not to contact you in this way. We will provide a clear method for you to opt out. You can also contact us directly at any time to tell us not to send you any future marketing material.

Very occasionally we carry out a joint mailing with carefully selected other organisations, in order to tell you about products and services we think you might be interested in. Again, you have the right to opt out of this.

You have the right to a copy of all the information we hold about you (apart from a very few things which we may be obliged to withhold because they concern other people as well as you). To obtain a copy, either ask for an application form to be sent to you, or write to the Data Protection Officer at Supplytrain <add email address here?>. There is a charge of £10 for a copy of your data (as permitted by law). We aim to reply as promptly as we can and, in any case, within the legal maximum of 40 days.

Appendix B: Confidentiality statement for staff and contractors

When working for Supplytrain, you will often need to have access to confidential information which may include, for example:

- Personal information about individuals who are work scheme participants or otherwise involved in the activities organised by Supplytrain.
- Information about the internal business of Supplytrain.
- Personal information about colleagues working for Supplytrain.

Supplytrain is committed to keeping this information confidential, in order to protect people and Supplytrain itself. 'Confidential' means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the Data Protection Act, unauthorised access to data about individuals is a criminal offence.

You must assume that information is confidential unless you know that it is intended by Supplytrain to be made public.

You must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:

- not compromise or seek to evade security measures (including computer passwords);
- not gossip about confidential information, either with colleagues or people outside Supplytrain;
- not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised to have it.

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped working for Supplytrain.

I have read and understand the above statement and Supplytrain's Data Protection Policy. I accept my responsibilities regarding confidentiality.

Signed: **Date:**