Young Enterprise Data Protection Policy

1. What does this policy cover?

Young Enterprise Group (**"Young Enterprise", "we", "us", "our**") is committed to handling personal information about individuals, including its employees, volunteers, contractors, programme and service users, supporters and suppliers, in accordance with the law that applies to us in the countries in which we operate.

This Data Protection Policy (the "**Policy**") sets out how Young Enterprise members of staff (including employees, temporary and contract staff) and volunteers must handle personal information. Complying with this Policy is a requirement for all Young Enterprise members of staff and volunteers who handle or have access to personal information in their day-to-day role, even if such access is not part of their core tasks. The Annex defines the key terms used in this Policy.

This Policy sits alongside other policies which relate to the processing of personal information by Young Enterprise and should be read together with those policies available on YE's SharePoint in the Data Protection Folder. It applies in addition to any confidentiality or professional obligations which are owned by Young Enterprise. If members of staff are unsure about what other internal Young Enterprise policies may be relevant to your role, please contact any member of YE's Senior Leadership Group. If volunteers are unsure about what other Young Enterprise policies are relevant to your role, please contact your Young Enterprise Area Manager in the first instance.

2. Why is this policy important?

The use of personal information is subject to rules and restrictions set out in privacy and data protection laws that we must comply with. Young Enterprise is committed to handling personal information properly and regards the lawful use of the personal information that it holds as vital to its successful operations.

Every member of staff and volunteer has a crucial role in making this happen, and this Policy explains what you need to do. If members of staff have any questions regarding this Policy, please speak to your line manager or any member of YE's Senior Leadership Group. If volunteers have any questions, please speak to your Young Enterprise Area Manager in the first instance.

Each member of staff is responsible for ensuring that Young Enterprise policies, standards and procedures, including this Policy, are followed in all cases. Please see section 6 'Enforcement' regarding the consequences of failing to comply with this Policy.

3. Types of personal information within the scope of this Policy

This Policy applies to all personal information that we process in the course of Young Enterprise operations, such as:

- Employee & volunteer data, including personal information about past and current employees, individual consultants, independent contractors, temporary staff, volunteers and job applicants.
- Young persons' data, including personal information about participants in our projects and programmes who use our websites, apps, products and services.
- Supply chain management data, including personal information about individual contractors, account managers and staff of third party suppliers who provide services to us or who we partner with.
- Donor and Supporter information including personal information about employees of supporters and prospective supporters who fund our work or who we partner with
- Teacher data, including personal information about teachers who engage with YE in our projects and programmes and who use our website, apps, products and services.
- Young Enterprise Alumni, including personal information about individuals who have participated in our programmes who are interested in keeping up to date with our work.
- Policy and campaigning, including personal information about members and supporters of the All Party Parliamentary Group on Financial Education for Young People, Financial Education Forum members, journalists and other stakeholders who have registered their interest in being kept informed of our policy and campaigning work or who have publicly expressed an interest in enterprise and financial education.

4. Legal standards

Young Enterprise operations are based in the UK and Young Enterprise will comply with the General Data Protection Regulation 2016/679 ("**GDPR**") and the UK Data Protection Act and other related regulations including the Privacy and Electronic Communications Regulations 2003. In addition to complying with privacy and data protection laws, for the Group's processing of personal data to be lawful it must comply with any other relevant legal requirements, including employment law.

4.1 Compliance with the law

Young Enterprise will process personal information on the basis of one of the legal grounds set out in data protection laws.

The law lists a number of grounds on the basis of which we may process personal information. Young Enterprise must only process personal information on the basis of one of those grounds, for instance, it is in our legitimate interests to process it (and there are no overriding rights of the data subjects) ; processing is necessary to perform a contract we have with the individual (for example, our obligation to pay an employee their salary); or we have obtained the consent of the data subject (for example, to send an individual marketing by e-mail).

4.2 Notice

Young Enterprise will explain to individuals, at the time their personal information is collected, how that information will be used and provide the information required by law.

We must ensure that we are transparent with individuals regarding why and how we process personal information about them. We will ensure this by providing notice to individuals. The notice must be readily available, must be clear and concise and must be easy to understand and access. Notice can be provided in different ways, including in writing and by electronic means, depending on the context. In limited cases we may not need to provide a notice, for example

because the individual already has the information or providing the notice may prove impossible or involve a disproportionate effort.

All notices provided to individuals must be reviewed and approved by the Senior Leadership Group when required. Please speak to any member of the Senior Leadership Group when considering any change to our operations which will result in us collecting personal information (either directly from individuals or from third parties e.g. purchasing marketing lists or developing new websites or apps).

4.3 Sensitive personal information

Young Enterprise will not process sensitive personal information unless the higher standards imposed by applicable law have been met.

Young Enterprise may process sensitive personal information, such as health data, racial/ethnic origin data, trade union membership, biometric data, genetic data or data about sex life or sexual orientation. For example, the processing of sensitive personal information may be required in order for Young Enterprise to discharge its legal obligations (e.g. in respect of equality and diversity reporting).

The law sets out higher standards for processing sensitive personal information and also any information regarding an individual's criminal convictions (for example, where we request a DBS check in respect of a member of staff or volunteer who will work with children and young people). Young Enterprise's processing of sensitive personal information and criminal convictions data will trigger additional requirements, such as carrying out a Data Protection Impact Assessment ("DPIA") to assess the implications of collecting and processing these types of information and how Young Enterprise will comply with legal requirements. Speak to the Senior Leadership Group if you are thinking of processing sensitive personal information and **always do so before** collecting any information.

4.4 Accountability

Young Enterprise must be able to demonstrate that it complies with data protection law.

Young Enterprise is responsible for compliance with data protection law when processing personal data. It is not enough to be compliant, we must also be able to evidence how we ensure compliance.

Young Enterprise is required to take several steps to comply with the Accountability principle. These include a data protection governance framework; identifying clear lines of responsibility for data protection compliance; carrying out Data Protection Impact Assessments ("DPIAs") where applicable and data protection audits; and rolling out data protection training to all members of staff.

Young Enterprise members of staff play a crucial role in enabling Young Enterprise to comply with the Accountability principle, for instance by carrying out DPIAs, participating in data protection audits or reviews, documenting Young Enterprise's data processing activities, keeping data processing records and data flow maps. Young Enterprise expects full cooperation from members of staff when they are required to take part in these activities. For instance, if you are planning a new project, you may be asked to provide the information required for a DPIA; you may also be asked to fill in an audit questionnaire, keep records of data processing activities or provide the information required to create a data map (e.g. if the data is transferred to or accessed by third parties).

4.5 Privacy by Design and Privacy by Default

Young Enterprise must ensure privacy is considered at the beginning of the data protecting activities, and that by default it only processes the minimum of personal data necessary to achieve the intended purpose.

Young Enterprise must ensure that adequate technical measures (such as technology and software solutions) and organisational measures (such as policies, processes and controls) for privacy protection are in place from the start of each data processing activity. In other words, we must ensure that for each new technology, project, campaign or other data processing activity, appropriate privacy controls are 'baked in' by design, as opposed to being an afterthought (e.g. if we launch new websites or apps; if we purchase marketing lists or if we start to use personal information for new purposes, share it with new providers or change the locations in which personal information is processed). Young Enterprise must also ensure that it only processes the minimum personal information that is necessary to achieve the intended business purpose and that appropriate security and privacy controls are applied during the entire data processing lifecycle. Running DPIAs at the beginning of a new activity is the main tool we have to embed privacy by design and by default into our activities.

4.6 Purpose limitation

Young Enterprise will only use the personal information it collects for specified, explicit and legitimate purposes that it has explained to individuals, and will not further process personal information in a way that is incompatible with the purposes for which it was originally collected.

In practice, this means that we must always have a clear purpose for which we collect personal information and only use it for that purpose and compatible purposes. If you wish to process personal information for an additional purpose that you did not anticipate when you collected it, please contact the Senior Leadership Group as required. They will help you assess whether the fresh purpose is compatible with the purpose for which the personal information was obtained and, in any event, what we need to do in order to achieve the objective.

4.7 Data minimisation

Young Enterprise will only collect personal information that is adequate, relevant and the minimum necessary for the intended purposes.

In practice, this means that we must be clear regarding what personal information we need to achieve our purpose and ensure that we only collect that minimum information. We must not collect personal information 'just in case' it may be needed in the future or because it is 'nice to have'. In addition to being unlawful, collecting unnecessary information has costs and data security risk implications for Young Enterprise. Please speak to the Senior Leadership Group **before** you start collecting personal data using new processes (e.g.through new websites or apps or buying-in marketing lists), who will help you ensure that you only collect the personal information that you need.

4.8 Accuracy

Young Enterprise must take appropriate measures to ensure that the personal information that we process is accurate and, where necessary, kept up to date.

We must carry out regular checks to ensure the accuracy of the personal information that we hold, including sending reminders to individuals to keep the information in their records or accounts up-to-date. You must contact Senior Leadership Group if you are unsure about the accuracy of a certain data set or if you suspect that the information may be out-of-date. An

example is a spreadsheet containing personal information of individuals who participated in, for instance, a marketing promotion two years ago or CVs and interview notes of candidates who were interviewed but not employed by Young Enterprise over 6 months ago.

4.9 Data retention

Young Enterprise must not keep personal information in a form which permits identification of individuals for longer than is necessary for the purposes for which that personal information is processed.

All personal information will be archived or deleted in accordance with our document retention and deletion policy.

4.10 Security, integrity and confidentiality

Young Enterprise will adopt and maintain appropriate technical and organisational security measures to ensure that personal information is not put at risk and is handled in accordance with our security standards.

Young Enterprise will apply appropriate security to protect personal information against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular when personal information is transmitted over a network, and against all other unlawful forms of processing. You should consult with our Senior Leadership Group for new projects that you are planning. For more information on Young Enterprise's security standards, please refer to the Young Enterprise Information Security Policy.

4.11 Data security incident reporting

Young Enterprise will deal with any security incidents and breaches in line with our incident report plan.

When required by law or when it is otherwise appropriate, Young Enterprise will notify data protection authorities of security breaches that put personal information at risk. In certain circumstances, Young Enterprise may also need to notify affected individuals. In addition, we may need to notify other external parties (such as notifying our advisors and insurers/brokers or liaising with the press).

Examples of breaches of personal information include the loss of a laptop containing personal information that is not sufficiently protected, the disclosure of personal information to an unauthorised person (e.g. because we accidentally sent them an email or gave them access to a database) or a cyber-attack during which personal information may be accessed.

You must immediately report internally (in accordance with Young Enterprise's Security Incident Management Policy) if you become aware of an incident or breach, or potential breach, that affects our systems or processes and puts personal information at risk of, for instance, accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Please report such an incident to Sharon Davies Deputy CEO on sharon.davies@y-e.org.uk or Michael Mercieca CEO on mm@y-e.org.uk and do not discuss this with anyone who does not need to know. For further information please refer to Young Enterprise's Security Incident Management Policy.

4.12 Using secure suppliers, vendors and data processors

When engaging vendors or service providers to process personal information on our behalf, Young Enterprise must use data processors that provide sufficient guarantees and only after signing appropriate contract terms.

Where we appoint a data processor (i.e. a vendor or service provider who processes personal information on our behalf, such as a marketing agency that will send promotional messages to individuals or the provider of a cloud-based CRM solution), we must ensure that they provide sufficient guarantees. There are three key things that we must do:

a) carry out pre-contractual due diligence checks (for instance, requiring copies of DPIA reports, data protection and security policies or that the processor fills in a due diligence questionnaire);
b) sign a written contract with appropriate data protection and data security terms; and
c) carry out reasonable post-contractual checks and/or audits to ensure that the data processor complies with the contract.

If you are thinking of engaging a data processor, you must contact the Senior Leadership Group prior to making any commitment.

4.13 Individuals' rights

Data subjects have several rights concerning the personal information that Young Enterprise processes about them. Young Enterprise respects these' rights and will honour requests swiftly and in accordance with legal requirements.

- **The right of access**: individuals may obtain confirmation of whether we process personal information about them and be provided with details of that personal information and access to it.

- **The right to rectification**: individuals may require us to rectify any inaccurate personal information that we process about them.

- **The right to erasure**: individuals may require us to erase personal information about them on certain grounds.

- **The right to restriction**: individuals may require us to restrict the processing of personal information about them on certain grounds.

- **The right to data portability**: individuals may request to receive certain personal information concerning them in a structured, commonly used and machine-readable format and to transmit that information to another company, if certain grounds apply.

- **The right to object**: individuals may object to the processing of personal information about them, if certain grounds apply.

- **The right to object to direct marketing**: individuals may object, free of charge, to the use of their personal information for direct marketing purposes.

Young Enterprise must deal with such requests swiftly and effectively, within the tight timeframes required by law, even if they are not submitted through the right channel. The Senior Leadership Group will deal with such requests. If you receive a request or complaint concerning personal information, immediately inform a member of the Senior Leadership Group.

4.14 Data exports

Young Enterprise will not transfer personal information to (or grant access to personal information from) other countries unless appropriate measures have been implemented to protect it.

Personal information must not be transferred outside of the EEA unless appropriate steps are taken to ensure that it remains protected to the same standards.

If you are planning to transfer personal information outside the EEA, please contact the Senior Leadership Group. (You must do the same if you plan to grant remote access to the personal information from another country or from outside the EEA.) They will be able to advise you what measures need to be put in place to ensure that data exports are lawful.

4.15 Disclosure of personal information

Young Enterprise will control the disclosure of personal information and ensure that any disclosures are lawful.

Young Enterprise will disclose personal information to third parties or law enforcement agencies where we are required or allowed by law to make such disclosures. If you receive a request to disclose personal information from a public authority, government agency, a third party outside Young Enterprise, please contact the Senior Leadership Group prior to making any information available.

4.16 Automated decision making and profiling

Young Enterprise must respect the right of data subjects not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects or similarly significantly affects them.

If you are planning to process personal information for automated decision making or profiling purposes, please contact Senior Leadership Group to advise on what steps must be taken to ensure this is done lawfully. In some cases, such as when automated processing or profiling has *'legal effects'* or *'similarly significantly affects'* individuals, Young Enterprise may need explicit consent from individuals, so it is crucial that you involve the Senior Leadership Group as soon as possible.

5. Privacy investigations and dispute resolution

We will address complaints or disputes regarding the processing of personal information promptly and in accordance with applicable law. Where appropriate, we will cooperate with privacy regulators in the investigation and resolution of complaints and will seek to comply in good faith with their advice.

6. Enforcement

Failure to comply with privacy and data protection laws can lead to serious consequences for Young Enterprise including a loss of reputation and trust, regulatory audits, massive fines, lawsuits and criminal sanctions. All members of staff and volunteers must comply with this Policy.

Breach of the Policy by a member of staff may lead to disciplinary action and, in serious cases (such as a conscious misuse or theft), may lead to dismissal. Please also note that in some cases, the unauthorised use of personal information can lead to personal liability and can constitute a criminal offence (for example, where an employee brings a list of customer/supplier contacts from a previous employer or takes this information from Young Enterprise's systems to a new employer).

7. Changes to this Policy

Young Enterprise may update this Policy from time to time to reflect changes in the applicable law and/or our practices. Changes to this Policy will be notified to members of staff and volunteers via the regular channels. Additional training will be provided where necessary.

Annex: Key data protection terms

Below is the meaning of certain key terms used throughout this Policy.

- **data subject (or individual)** means the identified or identifiable natural person to whom the personal information relates. Any individual about whom Young Enterprise processes data is a data subject. For instance, this would typically be an Young Enterprise participant, member of staff/volunteer, contractor or supplier.

- **personal information** means any information relating to an identified or identifiable natural person. An identifiable natural personal 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 nature personal – it can include contact details, transaction history, financial details for individuals, CCTV images of individuals, visitor/staff sign-in details, online behavioural linked to devices/IP addresses – if in doubt, it is safest to assume that it is personal data and within the scope of this Policy;

- **processing** means any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Pretty much anything Young Enterprise does with personal information is 'processing';

- **sensitive personal information** means information that relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. It also includes information about an individual's criminal offences or convictions, as well as any other information deemed sensitive under applicable data protection laws.