Data Protection Policy

Reviewed and adopted by the Board of Trustees: 11th September 2023

Next Review Date Q3 2024

Data Protection Policy

Construction Youth Trust Ltd (hereinafter referred to as 'the Trust') is fully committed to a policy of protecting the rights and privacy of individuals in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (the DPA). The Trust considers that the correct treatment of personal data is integral to successful operations. Non- compliance with the data protection requirements outlined in this policy will expose the Trust to complaints, regulatory actions, fines and/or reputational damage.

This policy sets forth the expected behaviours of trustees, employees, funders, business contacts, beneficiaries, contractors/consultants and other third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data. Any breach of this policy will be taken seriously.

1. Scope

1.1 This policy applies to all Trust entities where a data subject's personal data is processed:

- In the context of the business activities of the Trust
- To fulfil an agreement/contract
- For the provision or offer of goods or services to individuals (including those provided or offered free-of-charge)
- To actively monitor the behaviour of individuals when required by the Client.

1.2 This policy applies to all processing of personal data by the Trust falling within the scope of the UK GDPR and the DPA in all formats including paper, electronic, audio and visual.

2. Personal and special category data

2.1 The UK GDPR and DPA provides conditions for the collecting and processing of any personal data. It also makes a distinction between personal data and 'special category' personal data**.**

2.2 Personal data means 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.

2.3 Special category personal data is defined as personal data consisting of information as to:

- racial or ethnic origin;
- political opinion;
- religious or other beliefs;
- trade union membership;
- physical or mental health or condition;

- sexual life or sexual orientation;
- genetics
- biometric data (where used for id purposes)

2.4 Although there are clear distinctions between personal and special category data for the purposes of this policy the term '*personal data'* refers equally to '*special category data'* unless otherwise stated.

2.5 The UK GDPR and DPA rules for special category data do not apply to information about criminal allegations, proceedings, or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures.

3. Personal data processed by the Trust

3.1 The Trust processes personal data to provide a service. Personal data must be handled and dealt with in accordance with the UK GDPR, DPA and this policy. There are safeguards within the UK GDPR and DPA to ensure personal information is collected, recorded and used whether it is on paper, computer records or recorded by any other means.

3.2 The obligations outlined in this policy apply to everyone who has access to, holds copies of or processes personal data. This includes those who work at/from home or have remote or flexible patterns of working.

4. Data controller

4.1 The data controller is the person who (either alone or jointly or in common with other persons) determines the purposes for which and means of the processing of personal data.

4.2 Construction Youth Trust Ltd is the data Controller for all personal data relating to its young people, children/students, relatives, volunteers, staff and any other individual.

5. Roles and responsibilities

5.1 This policy applies to all staff employed by the Trust. Staff who do not comply with this policy may face disciplinary action.

5.2 The Board of Trustees

The Board of Trustees of Construction Youth Trust are ultimately responsible for ensuring that the Trust meets it legal obligations, delegating day to day responsibility for managing these risks to the Chief Executive.

5.3 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, developing related

policies and guidelines where applicable and for the following:

- Keeping the Chief Executive and the Board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related policies, in line with an agreed schedule
- Arranging data protection training and advice for the individuals covered by this policy
- Handling data protection questions from all individuals covered by this policy
- Dealing with requests from individuals that the Trust holds about them
- Checking and approving any contracts or agreements with third parties that may handle the Trust's sensitive data
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Monitor staff compliance with Data Protection Legislation by carrying out regular reviews which includes the effectiveness of handling, processing activities and security controls.

The Data Protection Officer is also the first point of contact for individuals whose data the Trust processes and for the Information Commissioner's Office.

Our Data Protection Officer is our Data & IT Manager Conor Baigent

5.4 Head of Central Resources

The Head of Central Resources is responsible for:

- Approving any data protection statements attached to communications such as emails and letters
- Addressing any data protection queries from journalists or media outlets
- Where necessary working with other staff to ensure marketing initiatives comply with data protection legislation

5.5 All Staff

All Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy;
- Informing us of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If you have concerns that this policy is not being followed
  - If you are unsure whether or not you have a lawful basis to use personal data in a particular way
  - If you need to rely on or capture consent, deal with the rights of the data subjects or transfer personal data outside the UK
  - If there has been a data breach
  - Whether you are engaging in a new activity that may affect the privacy rights of individuals

- If you need help with any contracts or sharing personal data with third parties

6. Data protection principles

6.1 Article 5 (1) of the UK GDPR sets out seven key principles. Anyone processing personal data must comply with the data protection principles which govern the Trust's collection, use, retention, transfer, disclosure and destruction of personal data.

These principles are legally enforceable and are summarised as follows:-

- **Principle 1: Lawfulness, Fairness and Transparency**

  Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

  This means:

  - Transparency - the Trust must tell the Data Subject what Processing will occur.
  - Fairness - the Processing must match the description given to the Data Subject.
  - Lawfulness - It must be for one of the purposes specified in the applicable Data Protection regulation.

- **Principle 2: Purpose Limitation**

  Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes.

  This means the Trust must specify exactly what the personal data collected will be used for and limit the Processing of that personal data to only what is necessary to meet the specified purpose.

- **Principle 3: Data Minimisation**

  Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed.

  This means the Trust must not store any personal data beyond what is strictly required.

- **Principle 4: Accuracy**

  Personal Data shall be accurate and, kept up to date.

This means the Trust must have in place processes for identifying and addressing out-of- date, incorrect and redundant personal data.

- **Principle 5: Storage Limitation**

  Personal Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

  This means the Trust must, wherever possible, store personal data in a way that limits or prevents identification of the data subject or securely destroy the personal data when no longer required.

- **Principle 6: Integrity & Confidentiality**

  Personal Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

  The Trust must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained always.

  Article 5(2) adds:

- **Principle 7: Accountability**

  The Controller shall be responsible for and be able to demonstrate compliance.

  This means the Trust must demonstrate that the Data Protection Principles (outlined above) are met for all personal data for which it is responsible.

7. Notification

7.1 The national body for the supervision of the UK GDPR is the Information Commissioners' Office (ICO) to whom the Trust notifies the purposes for processing personal data.

7.2 This notification process serves to provide transparency and openness about the processing of personal data. It is a fundamental principle of the UK GDPR that the public should know or be able to find out who is carrying out the processing of personal data and for what purpose.

7.3 The Trust's registration number with the ICO is Z2890294. A copy of the Trust's notification details is available on the Information Commissioner's website

8. Individual rights

8.1 The Trust recognises that access to personal data held about an individual is a fundamental right provided in the Act.

8.2 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Trust holds about them. To minimise delays and unnecessary work all requests from data subjects should meet the requirements stated in the Trust's Subject Access Policy.

9. Data processing

9.1 The Trust uses the Personal Data for the following broad purposes:

- To provide services
- The ongoing administration and management of beneficiary and partner relationships
- To fulfil the contract/agreement between the Trust and a partner

9.2 The use of a beneficiary or partner's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

9.3 For example, it would clearly be within a beneficiary or partner's expectations that their details will be used by the Trust to provide a service. However, it will not be within their reasonable expectations that the Trust would then provide their details to Third Parties for marketing purposes.

9.4 The Trust will process personal data in accordance with all applicable laws and contractual obligations. More specifically, the Trust will not process personal data unless at least one of the following requirements are met:

- The Data Subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child)

10. Law enforcement requests and disclosures

10.1 In certain circumstances, it is permitted that personal data can be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders

- The assessment or collection of a tax or duty
- By the order of a court or by any rule of law.

10.2 If the Trust processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

11. Data security

11.1 The Trust has physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by human action or the physical or natural environment.

A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data being transmitted electronically during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that personal data is protected against undesired or accidental destruction, damage or loss.
- Ensure that personal data is not kept longer than necessary

11.2 All printout material, magnetic tape, diskettes, CD's or DVD's, manual files, handwritten notes etc, which contain personal data and are no longer required, will be treated as confidential waste and disposed of securely.

11.3 Where processing of Trust data is to be carried out by a third party on behalf of the Trust, the Trust must ensure that the third party provides sufficient guarantees in respect of the technical and organisation measures governing the processing to be undertaken.

11.4 The Trust shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the Trust's property without permission from the Data & IT Manager. Users breaching this requirement may be subject to disciplinary action.

11.5 Email poses a significant threat and files attached to and links within email must be treated with caution to safeguard against Phishing type attacks which seek to harvest personal information and deliver malicious code including ransomware that can lead to the encryption of important Trust data. All staff have a duty to check the address of the recipient each time an email is sent to reduce the chance of accidental data loss through email.

11.6 The use of USB storage devices is a common cause of compromise through infections from computer viruses, malware and spyware and should be avoided.

12. Profiling and automated decision-making

12.1 The Trust will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform, a contract where it is authorised by law.

12.2 Where the Trust utilises profiling and automated decision-making, this will be disclosed to the Data Subject.

12.3 It should be remembered that in such cases the Data Subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.
- Object to the automated decision-making being carried out.

12.4 The Trust must also ensure that all profiling and automated decision-making relating to a Data Subject is based on accurate data.

13. Data retention

13.1 To ensure fair Processing, personal data will not be retained by the Trust for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed.

13.2 All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

14. Data transfer

14.1 The Trust may transfer personal data to internal or third-party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects.

14.2 Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism. The Trust may only transfer personal data where one of the transfer scenarios listed below applies:

- The transfer is necessary for the performance of a contract.
- The transfer is necessary for the implementation of pre-contractual measures taken in response to a partner's request
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third-Party in the interest of a partner
- The transfer is legally required on important public interest grounds

- The transfer is necessary for the establishment, exercise or defence of legal claims
- The transfer is necessary to protect the vital interests of the data subject

15. Data protection by design and default

15.1 The Trust will use a Data Protection Impact Assessment (DPIA) toolkit to evaluate all new systems to help determine how data protection compliance can be assured.

15.2 DPIA toolkits provide a step-by-step approach to evaluate new or existing information systems for compliance with the legislation. The DPIA process helps to identify weaknesses or risks to data losses or breaches and consider action that needs to be taken to ensure compliance where such compliance is not yet achieved. DPIA applies equally to paper as well as electronic data holding systems.

16. Personal data breaches

16.1 The Trust will make all reasonable endeavours to ensure that there are no personal data breaches

16.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g., financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Trust will inform the Client without delay, and in any event, within 24 hours after having become aware of it.

17. Training and awareness

17.1 Data protection training and awareness are crucial to ensure all staff understand their responsibilities in relation to data protection and the use of personal data. Failure to comply with the UK GDPR, DPA and the Principles could lead to serious problems, and in some cases may result in significant fines or criminal prosecution.

17.2 It is the Trust's policy to ensure that the applicable training course is completed annually.

18. Policy review

18.1 This policy will be reviewed every two years. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

19. Links with other policies

19.1 This Data Protection policy is linked to the Trust's:

- Privacy Notice
- Data Protection Impact Assessment Policy
- Security Incident and Data Breach Policy

- Information Security Policy
- Subject Access Request Policy
- Safeguarding Policy

19.2 The ICO also provides a free helpdesk that can be used by anyone and a website containing a large range of resources and guidance on all aspects of Information Law for use by organisations and the public. See www.ico.org.uk

Appendix 1

ESF Compliance

For data relating to the ESF Careers Cluster programme, this will be kept for 10 years after the date of the final ESF claim is paid by the ESF Managing Authority.

This will include the following documents to be kept on Record for this Timeframe:

- All ESF related documentation including work carried out during the development, pre application, application and during and after the project;
- The Funding Agreement including any revised versions supported by appropriate correspondence from DWP of the approval of changes to the Funding Agreement;
- Correspondence from/to the Managing Authority;
- Quarterly or monthly claim forms;
- Working papers showing how claims were calculated, including any flat rate methodologies;
- The audit trail for all procurement undertaken for the project; and
- The State Aid approved scheme used where relevant.

The following documents will also be kept for this duration:

- Evidence of all project expenditure. This include invoices and bank statements or equivalent.
- Calculations for indirect overheads costs and salaries for the project, as well as the agreed methodology for calculating these costs;
- Records of eligible participants and any supporting evidence to confirm their eligibility to receive ESF support;
- Evidence of open and fair procurement of goods and services. Including proof of advertising and contract notices, quotations or tenders received and the scoring methodology used for selecting the successful candidate. This will include details of all preparatory work prior to the procurement process and the delivery/use of the procured service and goods.
- Evidence of auditable, accountable match funding, including copies of match funding acceptance letters and bank statements showing receipt of match funding;
- Compliance with publicity requirements. Copies of all publicity materials, including press releases and marketing will be retained to demonstrate the correct use of the EU logo and required text.
- Compliance with equal opportunities and environmental sustainability requirements;
- Clear records of businesses supported for state aid purposes, including signed declarations where an organisation is operating under any state aid rules, such as de minimis, or any other state aid ruling;
- Documentary evidence substantiating the outputs and results declared in ESF claims and on completion of projects;
- A record of the identity and location of all bodies holding the supporting ESF project documentation, to be made available on request to the Managing and Audit Authorities.