Subject Access Request Policy

Reviewed and adopted by the Board of Trustees: 11th of September 2023
Next Review Date: Q3 2024

Subject Access Request Policy

The GDPR and DPA 2018 gives individuals the right of access to their personal information held by Construction Youth Trust (the Trust). Subject access is a fundamental right for individuals, but it is also an opportunity for the Trust to provide excellent customer service by responding to Subject Access Requests (SARs) efficiently and transparently and by maximizing the quality of the personal information you hold. This Policy explains how the Trust will fulfil its obligations under the Act.

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with the principles (Article 5(1) of the GDPR), which make sure that personal information is:

- processed lawfully, fairly and in a transparent manner
- collected and processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant, and limited to what is necessary for the purpose
- Accurate and kept up to date
- Not kept for longer than is necessary and subject to appropriate technical and organisation measures to safeguard the rights and freedoms of individuals
- processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing; and

Article 5(2) adds that 'the controller shall be responsible for, and be able to demonstrate compliance with Article 5(1) ('accountability') and;

Secondly, it provides individuals with important rights (Articles 13 and 14):

1) Right to be informed
2) Right of access
3) Right to rectification
4) Right to erasure (right to be forgotten)
5) Right to restrict processing
6) Right to data portability
7) Right to object
8) Rights related to automated decision making including profiling

This policy will be reviewed annually.

1. Purpose

1.1 The aim of this policy is to ensure that the Trust complies with its legal obligations under the General Data Protection Regulation and Data Protection Act 2018 and can evidence that the Trust have done so. It also aims to ensure that the Trust:

- has robust processes in place for dealing with SARs, saving time and effort
- increases levels of trust and confidence by being open with individuals about the personal information the Trust holds
- improves the transparency of Trust activities in line with public policy requirements

1.2 This Policy outlines how an applicant can make a request for their personal information under the Act and how it will be processed. This is not a legal document. It does not confer rights nor override any legal or statutory provisions which either require or prevent disclosure of personal information, rather this document considers the key features of the Act and outlines how the Trust will take steps to ensure compliance in relation to requests for personal information.

1.3 Requests for access to the records of people who are deceased are not within scope of this Policy as the Act only applies to the data of living individuals. Such requests will be treated as requests for access to information under the Freedom of Information Act or as miscellaneous requests, depending on the nature of the data and the reason the data is being requested.

1.4 Subject access is most often used by individuals who want to see a copy of the information the Trust holds about them. However, subject access goes further than this and an individual is entitled to be:

- Told whether any personal data is being processed
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
- Given a copy of the personal data
- Given details of the source of the data (where this is available)

1.5 An individual can also request information about the reasoning behind any automated decisions taken about him or her, such as a computer-generated decision for assessment of performance at work.

1.6 This policy should be read in conjunction with the Subject Access Request Procedure, please see the Staff Handbook.

2. General policy on providing information

2.1 The Trust welcomes the rights of access to information that are set out in the GDPR and DPA. The Trust is committed to operating openly and to meeting all reasonable requests for information that are not subject to specific exemptions in the Act.

2.2 Subject Access requests fall within the data protection statutory framework and the ability to identify and appropriately handle a request for information is considered to be part of every employee's role.

2.3 Your primary responsibility is to ensure that Subject Access Requests are in the first instance directed to the Trust's Data Protection Officer. It is important that requests are processed as soon as they are received to assist in meeting the statutory deadline.

3. Individuals making a subject access request

3.1 A subject access request is a written request for personal information (known as personal data) held about an individual by the Trust. Generally, all individuals have the right to see what personal information the Trust holds about them and is entitled to be given a description of the information, what the Trust uses it for, who the Trust might pass it onto, and any information the Trust might have about the source of the information. However, this right is subject to certain exemptions that are set out in the GDPR and DPA.

3.2 A valid subject access request should be made in writing via email to

dpo@constructionyouth.org.uk or by post to the Data Protection Officer at the Trust address. Individuals may make a subject access request using any Facebook page or Twitter account that the Trust has, but this is not recommended.

3.3 The Trust may require individuals to complete a request form to ensure the Trust has all the details needed to locate the information required, but the Trust will not use this as a way of extending the time limit for responding.

4. Subject access request process

4.1 Checking of Identity

4.1.1 The Trust will first check that there is enough information to be sure of an individual's identity.

4.1.2 If the person requesting the information is a relative/representative of the individual concerned, then the relative/representative is entitled to personal data about themselves but must supply the individual's consent for the release of their personal data. If an individual has been appointed to act for someone under the Mental Capacity Act 2005, they must confirm their capacity to act on the individual's behalf and explain how they are entitled to access the requested information.

If the request is made by a parent/guardian of a child under 16, the Trust will need to consider:-

- Where possible, the child's level of maturity and their ability to make decisions
- The nature of the personal data
- Any court orders relating to parental access or responsibility that may apply
- Any duty of confidence owed to the child or young person
- Any consequences of allowing those with parental responsibility access to the child's or young person's information, particularly important if there have been allegations of abuse or ill treatment
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- Any views the child or young person has on whether their parents should have access to information about them

4.1.3 Should an individual make a data subject access request but not be the data subject, they must stipulate the basis under the GDPR that they consider make them entitled to the information.

4.2 Collation of information

4.2.1 The Trust will check whether there is enough information to find the records requested. If the Trust needs more information, this will be promptly requested. The Trust will gather any manual or electronically held information and identify any information provided by a third party or which identifies a third party.

4.2.3 When responding to a subject access request that involves providing information that relates both to the individual making the request and to another individual the Trust do not have to comply with the request if to do so would mean disclosing information about another individual who can be identified from that information, except where:

- The other individual has consented to the disclosure; or

- It is reasonable in all the circumstances to comply with the request without that individual's consent

The Trust may sometimes be able to disclose information relating to a third party and the decision will be on a case by case basis. The decision to disclose will be based on balancing the data subject's right of access against the third party's individual rights in respect of their own personal data. If the third-party consents to disclosure, then it would be unreasonable not to do so. However, if there is no consent, the Trust will decide whether it is 'reasonable in all the circumstances' to disclose the information and will consider the following:-

- Is there any duty of confidentiality owed to the third-party;
- Any steps the Trust have taken to try and obtain third-party consent;
- Whether the third-party is capable of giving consent; and
- Any stated refusal of consent by the third-party.

4.2.4 Before sharing any information that relates to third parties, the Trust may anonymise information that identifies third parties not already known to the individual and edit information that might affect another party's privacy. The Trust may also summarise information rather than provide a copy of the whole document.

4.3 Issuing the Trust response

4.3.1 Once any queries around the information requested have been resolved, copies of the information in a permanent form will be sent except where agreed it is impossible or where it would involve undue effort. In these cases, an alternative would be to allow the information to be viewed on screen at the Trust's office.

4.3.2 The Trust will explain any complex terms or abbreviations contained within the information when it is shared.

5. Associated fees

5.1 The GDPR does not allow the Trust to charge a fee. However, the Trust can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive or when further copies are requested.

5.2 Where a request relates to 'unstructured person data' the Trust is not required to comply with the request if it estimates that the cost of doing so would exceed £450 (Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulation 2004)

6. Timelines

6.1 Any subject access request will be actioned within 28 days from when the Trust has received all the information necessary to identify an individual and to identify the information requested in order to provide the requested information or to provide an explanation about why the Trust is unable to provide the information.

6.2 However, there may be occasions where it is not possible to comply within 28 days if the request is:

- complex; or
- a number of requests have been received from an individual, including any other types of requests relating to individuals' rights. For example, if a SAR has been made in conjunction with a request for erasure and a request for data portability

simultaneously.

In such cases the Trust may extend the time limit by an additional 56 days to 84 days. Any extension would be communicated with an individual within 28 days of receiving the original request, with an explanation.

7. Previous requests and grounds for not complying with a subject access request

7.1 Previous request

If you have made a previous subject access request, the Trust must respond if a reasonable interval has elapsed since the previous request. A reasonable interval will be determined upon the nature of the information, the time that has elapsed, and the number of changes that have occurred to the information since the last request.

7.2 Exemptions

7.2.1 The Act contains a number of exemptions to the Trust's duty to disclose personal data. The Trust must consider whether it is possible to comply with the SAR without revealing information that relates to and identifies a third-party individual or any other exempt information.

Examples of third party information that cannot be shared routinely without specialist consideration are:

- Safeguarding concerns which may contain information about multiple children including siblings and estranged parents
- Files containing legally privileged information
- Files containing advice from relevant professionals such as doctors, police or probation services
- Employee files containing information identifying managers or colleagues who have contributed to (or are discussed in) that file.

Special consideration should be given to sharing this type of information.

8. Errors in Trust records

8.1 If the Trust agrees that the information is inaccurate, it will be corrected and where practicable, the inaccurate information destroyed. The Trust will consider informing any relevant third party of the correction.

8.2 If the Trust does not agree or feels unable to decide whether the information is inaccurate, the Trust will make a note of the alleged error and keep this on file.

9. Complaints procedure

9.1 In the first instance, complaints should be addressed with the Data Protection Officer and the Trust will review any written complaint about the way a request has been handled and about what information has been disclosed.

The Data Protection Officer can be contacted by email: dpo@constructionyouth.org.uk

9.2 If the Trust refuses to disclose information in response to a subject access request, the Trust may offer the applicant an opportunity to appeal the initial decision. If the applicant

believes that an error has been made in the response to their subject access request they are able to appeal the Trust's decision by seeking an internal review.

9.3 Once an appeal has been received the complainant will receive a written acknowledgement and the request and response to it will be reconsidered. The applicant will be notified of the outcomes of the internal review as soon as possible. All internal reviews should be concluded within 20 working days.

9.4 If an applicant's appeal is successful, they will receive the information they requested as soon as possible. If the appeal is unsuccessful the Trust will provide an explanation of the findings and supply further information on how to take the matter further.

9.5 If you remain dissatisfied with the outcomes of the Trust's decisions you have the right to refer the matter to the Information Commissioner's Office. The Information Commissioner's Office will make an initial assessment of the case before carrying out an investigation. The Information Commissioner's Office has written guidance notes for applicants on how to complain, published on their website. www.ico.org.uk

10. Links with other policies

This subject access request policy is linked to the Trust's:

- Data Protection Policy
- Security Incident and Data Breach Policy
- Records Retention Policy
- Information Sharing Policy
- Information Security Policy

Appendix 1

Dear [Requester],

I am writing in response to your subject access request dated [Date of request], which we received on [Date of receipt].

I would like to confirm that we have received your request and we will process it in accordance with the General Data Protection Regulation (GDPR). As a responsible data controller, we take data protection and privacy very seriously and we will ensure that your personal data is processed lawfully, fairly, and transparently.

In order to process your request, we will need to verify your identity to ensure that we are providing the personal data to the correct individual. We have sent this to the email address that we have on file for you, could you please respond confirming that you have requested this.

Once we have received and verified your identification, we will respond to your request within 30 days. We may require additional information from you to clarify your request, in which case we will contact you.

Please note that there may be circumstances where we are unable to provide you with all of the personal data that you have requested. This may be because the data is exempt from disclosure under the GDPR, or because providing the data would be disproportionate to the request. In such cases, we will explain why we cannot provide the data.

Thank you for your request, and please let us know if you have any questions.

Yours sincerely,