



Data Protection Policy

For Internal Use only:

Issue Number:	4.0
Reason for Issue:	Full review
Updated:	June 2024
Next Review:	June 2025
Written by:	Data Manager, Goodlaw Solicitors
Approved by:	Operations Manager (Projects)

Issue Log:

Issue Number:	Reason for Issue/Change:	Date:	Amended by:
4.0	Full review, reformatting	June 2024	Data Manager, Operations Manager

This policy gives important information about:

- the data protection principles with which Catalyst Support Limited (“Catalyst Support”) adhere to and to which employees must comply;
- what is meant by personal data (or information) and special category data (or information);
- how we gather, use and (ultimately) delete personal data and special category data in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal data we gather and use, how it is used, stored, and transferred, for what purposes, the steps taken to keep that data secure and for how long it is kept;
- individual rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

1 Introduction

- 1.1 Catalyst Support (hereafter also referred to as “the Charity”, “us”, “we”, or “our”) obtains, keeps, and uses personal data (also referred to as personal information) about job applicants and about current and former employees, temporary and agency workers, contractors, interns, volunteers, and apprentices, as well as about clients and users of Catalyst Support’s services and also individuals at organisations who deal with us. All the different types of personal data are processed for a number of specific lawful purposes in the management of Catalyst Support and the provision of charitable services.
- 1.2 This policy sets out how the charity complies with data protection obligations and seeks to protect all personal data. Its purpose is also to ensure that employees understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access in the course of their work.
- 1.3 This policy also provides a framework for ensuring that Catalyst Support meets its obligations under the UK General Data Protection Regulation and the Data Protection Act 2018.
- 1.4 Employees should refer to and be aware of Catalyst Support’s other relevant policies and guidelines which can be found in the Catalyst Support Employee Handbook, including the use of email and the internet, social media, information security, data

retention and the mobile device policy. These may provide further guidance which is relevant to the protection of personal data.

- 1.5 Catalyst Support are committed to complying with our data protection obligations, and to being concise, clear, and transparent about how we obtain and use personal data relating to our workforce, and how (and when) we delete that data once it is no longer required.
- 1.6 The Data Protection Lead is responsible for data protection compliance within Catalyst Support. If you have any questions or comments about the content of this policy or if you need further information, you should contact the Data Protection Lead by emailing dataprotection@catalystsupport.org.uk.
- 1.7 This policy does not form part of any employee's contract of employment, and we may amend, update, or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

2 Definitions

criminal records data	means personal data relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;
data subject	means the individual to whom the personal data relates;
personal data	(sometimes known as personal information) means data relating to an individual who can be identified (directly or indirectly) from that data;
processing data	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying data, or using or doing anything with it;
Pseudonymised	means the process by which personal data is processed in such a way that it cannot be used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual;

special category data (sometimes known as ‘special categories of personal data’, ‘sensitive personal data’ or ‘sensitive personal information’) means personal data about an individual’s race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics data, biometric data (where used to identify an individual) and data concerning an individual’s health, sex life or sexual orientation.

3 Data protection principles

3.1 Catalyst Support will comply with the following data protection principles when processing personal data:

- 3.1.1 we will process personal data lawfully, fairly and in a transparent manner;
- 3.1.2 we will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
- 3.1.3 we will only process the personal data that is adequate, relevant, and necessary for the relevant purposes;
- 3.1.4 we will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay;
- 3.1.5 we will keep personal data for no longer than is necessary for the purposes for which the data are processed; and
- 3.1.6 we will take appropriate technical and organisational measures to ensure that personal data are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

4 Basis for processing personal data

4.1 In relation to any processing activity, we will, before the processing starts for the first time, and then regularly while it continues:

- 4.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:
 - (a) that the data subject has consented to the processing;

- (b) that the 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;
 - (c) that the processing is necessary for compliance with a legal obligation to which Catalyst Support is subject;
 - (d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person;
 - (e) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or
 - (f) that the processing is necessary for the purposes of legitimate interests of Catalyst Support or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 4.2 below.
- 4.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
- 4.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
- 4.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices;
- 4.1.5 where 'special category data is processed, also identify a lawful special condition for processing that data (see paragraph 5.2.2 below), and document it; and
- 4.1.6 where criminal records data is processed, also identify a lawful condition for processing that data, and document it.
- 4.2 When determining whether Catalyst Supports' legitimate interests are the most appropriate basis for lawful processing, we will:
- 4.2.1 conduct a legitimate interest's assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
 - 4.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
 - 4.2.3 keep the LIA under review, and repeat it if circumstances change; and
 - 4.2.4 include information about our legitimate interests in our relevant privacy notices.

5 Special category data

5.1 Special category data is sometimes referred to as ‘sensitive personal data’ or ‘sensitive personal information.’

5.2 Catalyst Support may from time to time need to process special category data. We will only process special category data if:

5.2.1 we have a lawful basis for doing so as set out in paragraph 4.1.1 above, e.g. it is necessary for the performance of the employment contract, to comply with Catalyst Support’s legal obligations or for the purposes of Catalyst Support’s legitimate interests; and

5.2.2 one of the special conditions for processing special category data applies, e.g.:

- (a) the data subject has given explicit consent;
- (b) the processing is necessary for the purposes of exercising the employment law rights or obligations of Catalyst Support or the data subject;
- (c) the processing is necessary to protect the data subject’s vital interests, and the data subject is physically incapable of giving consent;
- (d) processing relates to personal data which are manifestly made public by the data subject;
- (e) the processing is necessary for the establishment, exercise, or defence of legal claims; or
- (f) the processing is necessary for reasons of substantial public interest.

5.3 Before processing any special category data, employees must notify the Data Protection Lead of the proposed processing, in order that an assessment may be carried out to determine whether the processing complies with the criteria noted above.

5.4 Special category data will not be processed until:

5.4.1 the assessment referred to in paragraph 5.3 has taken place; and

5.4.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

- 5.5 Catalyst Support will not carry out automated decision-making (including profiling) based on any individual's special category data.
- 5.6 Catalyst Support's privacy notice sets out the types of special category data that Catalyst Support processes, what it is used for and the lawful basis for the processing.
- 5.7 In relation to special category data, Catalyst Support will comply with the procedures set out in paragraphs 5.8 and 5.9 below to make sure that it complies with the data protection principles set out in paragraph 3 above.
- 5.8 During the recruitment process: the People and Culture team, with guidance from the Data Protection Lead will ensure that (except where the law permits otherwise):
 - 5.8.1 during the short-listing, interview and decision-making stages, no questions are asked relating to special category data, e.g. race or ethnic origin, trade union membership or health;
 - 5.8.2 if special category data is received, e.g. the applicant provides it without being asked for it within their CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted.
 - 5.8.3 any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing, or making the recruitment decision;
 - 5.8.4 'Right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview, or decision-making stages;
 - 5.8.5 we will only ask health questions once an offer of employment has been made
- 5.9 During employment: the People and Culture team, with guidance from the Data Protection Lead, will process:
 - 5.9.1 health data for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance, and facilitating employment-related health and sickness benefits;
 - 5.9.2 special category data for the purposes of equal opportunities monitoring and pay equality reporting. Where possible, this data will be anonymised; and

- 5.9.3 trade union membership data for the purposes of employee administration and administering 'check off.'

6 Criminal records data

Criminal records data will be processed in accordance with Catalyst Support's, convictions and offences policy, and Data retention in the employee handbook. This includes date of ref, name of subject and any disclosures.

7 Data protection impact assessments (DPIAs)

- 7.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where Catalyst Support is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

- 7.1.1 whether the processing is necessary and proportionate in relation to its purpose;

- 7.1.2 the risks to individuals; and

- 7.1.3 what measures can be put in place to address those risks and protect personal data.

- 7.2 Before any new form of technology is introduced, the manager responsible should therefore contact the Data Protection Lead in order that a DPIA can be carried out.

- 7.3 During the course of any DPIA, Catalyst will seek the advice of the Data Protection Lead and, as necessary, the views of relevant stakeholders.

8 Documentation and records

- 8.1 We will keep written records of processing activities, including:

- 8.1.1 the name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO);

- 8.1.2 the purposes of the processing;

- 8.1.3 a description of the categories of individuals and categories of personal data;

- 8.1.4 categories of recipients of personal data;

- 8.1.5 where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;

- 8.1.6 where possible, retention schedules; and
- 8.1.7 where possible, a description of technical and organisational security measures.
- 8.2 As part of our record of processing activities we document, or link to documentation, on:
 - 8.2.1 information required for privacy notices;
 - 8.2.2 records of consent;
 - 8.2.3 controller-processor contracts;
 - 8.2.4 the location of personal data;
 - 8.2.5 DPIAs; and
 - 8.2.6 records of data breaches.
- 8.3 If we process special category data or criminal records data, we will keep written records of:
 - 8.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
 - 8.3.2 the lawful basis for our processing; and
 - 8.3.3 whether we retain and erase the personal data in accordance with our policy document and, if not, the reasons for not following our policy.
- 8.4 We will conduct regular reviews of the personal data we process and update our documentation accordingly.

9 Privacy notice

- 9.1 Catalyst Support will issue privacy notices from time to time, informing you about the personal data that we collect and hold relating to you, how you can expect your personal data to be used and for what purposes.
- 9.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

10 Individual rights

10.1 You (in common with other data subjects) have the following rights in relation to your personal data:

10.1.1 to be informed about how, why and on what basis that data is processed;

10.1.2 to obtain confirmation that your data is being processed and to obtain access to it and certain other information, by making a data subject access request—see the Company’s subject access request policy;

10.1.3 to have data corrected if it is inaccurate or incomplete;

10.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as ‘the right to be forgotten’);

10.1.5 to restrict the processing of personal data where the accuracy of the data is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal data but you require the data to establish, exercise or defend a legal claim; and

10.1.6 to restrict the processing of personal data temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation’s legitimate grounds override your interests).

10.2 If you wish to exercise any of the rights in paragraphs 10.1.3 to 10.1.6, please contact the Data Protection Lead by emailing dataprotection@catalystsupport.org.uk.

11 Individual obligations

11.1 Employees, including volunteers, trustees, placements and contractors, (referred to as ‘you’) are responsible for helping Catalyst Support keep their personal data up to date. You have a responsibility for ensuring details in your HR profile are up to date. You should let the People and Culture team know if your account payroll details need to be updated or if there any other changes which cannot be updated through your HR profile.

11.2 You may have access to the personal data of other employees, suppliers, partners and clients of Catalyst Support in the course of your employment or engagement. If so, Catalyst Support expects you to help meet its data protection obligations to

those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 10.1 above.

- 11.3 If you have access to personal data, you must:
 - 11.3.1 only access the personal data that you have authority to access, and only for authorised purposes;
 - 11.3.2 only allow other Catalyst Support employees to access personal data if they need to do so as part of their job and they have appropriate authorisation;
 - 11.3.3 only allow individuals who are not Catalyst Support employees to access personal data if you have specific authority to do so from the individual whole personal data it relates to or from the Data Protection Lead;
 - 11.3.4 keep personal data secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction, complying with Catalyst Support's clear desk policy and other precautions set out in Catalyst Support's Employee Handbook);
 - 11.3.5 not remove personal data, or devices containing personal data (or which can be used to access it), or download personal data, from Catalyst Support's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the data and the device; and
 - 11.3.6 **not store personal data on local drives or on personal devices. Please also see the Catalyst Support Mobile device policy.**
- 11.4 You should contact the Data Protection Lead if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):
 - 11.4.1 processing of personal data without a lawful basis for its processing or, in the case of special category data, without one of the conditions in paragraph 5.2.2 being met;
 - 11.4.2 any data breach as set out in paragraph 14.1 below;
 - 11.4.3 access to personal data without the proper authorisation;
 - 11.4.4 personal data not kept or deleted securely;
 - 11.4.5 removal of personal data, or devices containing personal data (or which can be used to access it), from Catalyst Support's premises without appropriate security measures being in place;

11.4.6 any other breach of this policy or of any of the data protection principles set out in paragraph 3.1 above.

12 Information security

12.1 Catalyst Support will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage. These may include:

12.1.1 making sure that, where possible, personal data is pseudonymised or encrypted;

12.1.2 ensuring access is restricted so only employees who have a need to access personal data can do so, and limited to what they need in order to discharge their duties and obligations to Catalyst Support;

12.1.3 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

12.1.4 ensuring that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner;

12.1.5 ensuring that all staff and personnel are aware of this policy and have agreed to abide by it; and

12.1.6 a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

12.2 Where Catalyst Support uses external organisations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. In particular, contracts with external organisations must provide that:

12.2.1 the organisation may act only on the written instructions of Catalyst Support;

12.2.2 those processing the data are subject to a duty of confidence;

12.2.3 appropriate measures are taken to ensure the security of processing;

12.2.4 sub-contractors are only engaged with the prior consent of Catalyst Support and under a written contract;

- 12.2.5 the organisation will assist Catalyst Support in providing subject access and allowing individuals to exercise their rights in relation to data protection;
 - 12.2.6 the organisation will assist Catalyst Support in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
 - 12.2.7 the organisation will delete or return all personal data to Catalyst Support as requested at the end of the contract; and
 - 12.2.8 the organisation will submit to audits and inspections, provide Catalyst Support with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell Catalyst Support immediately if it is asked to do something infringing data protection law.
- 12.3 Before any new agreement involving the processing of personal data by an external organisation is entered into, or an existing agreement is altered, the relevant employees must seek approval of its terms by the Data Protection Lead.

13 Storage and retention of personal data

- 13.1 Personal data (and special category data) will be kept securely in accordance with Catalyst Support's Retention Policy.
- 13.2 Personal data (and special category data) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained.
- 13.3 Personal data (and special category data) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

14 Data breaches

- 14.1 A data breach may take many different forms, for example:
 - 14.1.1 loss or theft of data or equipment on which personal data is stored;
 - 14.1.2 unauthorised access to or use of personal data either by an employee or third party;
 - 14.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;
 - 14.1.4 human error, such as accidental deletion or alteration of data;

- 14.1.5 unforeseen circumstances, such as a fire or flood;
- 14.1.6 deliberate attacks on IT systems, such as hacking, viruses, or phishing scams;
and
- 14.1.7 'blagging' offences, where data is obtained by deceiving the organisation which holds it.

14.2 Catalyst Support will:

- 14.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- 14.2.2 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

15 International transfers

Catalyst Support will not transfer personal data outside the UK, or to international organisations, unless as part of relying on a third party supplier providing operational services or support to Catalyst Support and where the provision of such services or support cannot be accomplished without some processing of personal data outside the UK, in which case Catalyst Support shall ensure that the third party with access to the data has put in place adequate safeguards in accordance with data protection legislation.

16 Training

Catalyst Support will ensure that employees are adequately trained regarding their data protection responsibilities, and as part of their obligations to Catalyst Support all employees must ensure that they attend and complete all such training. 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.

17 Consequences of failing to comply

17.1 Catalyst Support takes compliance with this policy very seriously. Failure to comply with the policy:

- 17.1.1 puts at risk the individuals whose personal data is being processed; and

- 17.1.2 carries the risk of significant civil and criminal sanctions for the individual and Catalyst Support; and
- 17.1.3 may, in some circumstances, amount to a criminal offence by the individual.
- 17.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.
- 17.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact the Data Protection Lead by emailing dataprotection@catalystsupport.org.uk.

CONFIDENTIALITY PROCEDURES

- i) **General:** Personal data must be kept confidential at all times. It may only be shared between employees and volunteers for authorised purposes. In the event a situation arises which requires data to be shared outside Catalyst Support, for example with solicitors, police, social services, then speak to your line manager before doing so. Data cannot be shared unless appropriate consents are in place and approval from the Data Protection Lead has been obtained.
- ii) **New Clients:** All requests for any service offered by Catalyst Support should be treated as a new referral and before being referred to the appropriate employees consent for the sharing of personal data in the provision of services must be explained to and obtained from the individual, particularly where somebody may be contacting Catalyst Support on behalf of another person.
- iii) **Access and use of personal data:** It is a criminal offence to reveal personal data "knowingly" or "recklessly." Do not disclose or discuss confidential or personal information with anyone other than the individual themselves, unless permitted to do so.
- iv) All conversations should be held privately, and where that is not possible, please ensure confidential, personal, and special category data are not overheard by anyone who is not entitled to access such information. If you are outside your place of work, you must ensure you are not capable of being overheard or that sensitive information cannot be seen or accessed by another person.
- v) Take care of files, books, and other paper records as well as any electronic documents, to prevent unauthorised access and accidental loss or damage to confidential and personal information. Ensure all information is stored safely while working on it. Do not work in public areas or on public systems and

servers, or anywhere where it might be possible for somebody else to see or access your work.

vi) Use of email: Catalyst Support uses a password protected email system. Do not disclose your password to anyone else. If you believe somebody has access to your password, then notify the Data Protection Lead and arrange for your password to be changed.

vii) Catalyst Support also uses secure email encryption for the sending of confidential or sensitive information by email. You are responsible for ensuring the system updates are applied on your device.

viii) Disposal of documents: All documents containing confidential or personal information should be disposed of securely at work by shredding them so the document cannot be reconstituted. Documents should not be taken outside of the work place.

ix) Passwords: All Catalyst Support equipment is password protected. Do not disclose passwords for any device or system to anyone else, unless required to do so by Catalyst Support. Where you are required to change or update a password, do not keep it written down next to or together with the device. You are responsible for the safety and security of your password.

Once you have read and understood this policy, please confirm you that have done so by signing and returning the attached copy to Catalyst Supports’ appointed Data Protection Lead.

I have read and understood this policy and agree to abide by its terms.

Signed.....

Name.....

Date.....

This policy will be reviewed on an annual basis by the policy owner to ensure it remains up-to-date and fit for purpose.