POLICY
Data Protection

Date: [Feb 21]
Next review date: [Feb 22]

Contents

Introduction 1
Who this policy applies to 1
Responsible Officer 2
Application of this Policy 2
Lawfulness, fairness and transparency 3
Purpose Limitation 4
Data Minimisation 4
Accuracy 4
Storage Limitation 4
Security, Integrity and Confidentiality 6
Transfer Limitation 7
Data Subjects' rights and requests 7
Accountability 8
Direct marketing 9
Sharing Personal Data 9
Key terms 10
Changes to this Data Protection Policy 11
Acknowledgement 11

Introduction

Consortium's policy is to have the highest standards of data protection, in order to respect the right to confidentiality of our staff and all other people about whom we hold personal data for any reason.

Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. Please take the time to read and understand the policy. If you are a member of Consortium's staff, please ask your Line Manager any questions that arise from reading it. In any other cases, please contact our Responsible Officer, who leads on our data protection policy and compliance, at dp@consortium.lgbt.

This Policy reflects The Data Protection Act 2018, and other laws and regulations regarding data privacy in force in the United Kingdom. Consortium is registered with the Information Commissioners Office (ICO), which is an independent public authority set up to uphold information rights in the UK. Our registration number is ZA846350.

This policy uses certain terms that are defined by law. We have sought to use clear language as far as possible within this policy; however, we have used the legally defined terms for key terms. In the section '**Key terms**', you will find a glossary of these terms.

Who this policy applies to

This policy applies to all employees, workers, contractors, agency workers, consultants, volunteers, and trustees of Consortium ("**Consortium Personnel**", "**you**", "**your**", **"we"**). This Policy sets out what we

expect from you in order for Consortium to comply with applicable data protection law. You must read, understand and comply with this Policy when processing personal data on our behalf and attend training on its requirements. Your compliance with this Policy is mandatory, and any breach of this Policy may result in disciplinary action.

Responsible Officer

The Responsible Officer for this policy is the Chief Executive Officer. The Responsible Officer is the official Data Protection Officer (DPO) for Consortium. In their absence, the responsibility of this policy lies with the Head of Membership and Engagement. All enquiries about this policy and/or its application should be sent to dp@consortium.lgbt, which will automatically forward to the Responsible Officer.

It is the responsibility of the Responsible Officer to:

- ensure this policy is kept up to date;
- ensure that all appropriate data capturing procedures are in place;
- ensure that data is stored securely; and
- ensure requests for access to personal information are recorded.

Please contact the Responsible Officer with any questions about the operation of this Policy or if you have any concerns that this Policy is not being, or has not been, followed. In particular, you must always contact the Responsible Officer in the following circumstances:

- if someone wants to exercise their rights under data protection law regarding the Personal Data we hold about them;
- if you are unsure of the lawful basis which you are relying on to Process Personal Data (including the legitimate interests used by Consortium);
- if you need to draft Privacy Notices;
- if you are unsure about the retention period for the Personal Data being Processed;
- if you are unsure about what security or other measures you need to implement to protect Personal Data;
- if there has been, or you suspect, a Personal Data Breach;
- if you are sending Personal Data outside the European Economic Area;
- whenever you are engaging in a significant new Processing activity, significantly changing a current Processing activity, or plan to use Personal Data for purposes others than what it was collected for;
- If you plan to undertake any activities involving automated processing (where decisions are made on an automated basis);
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties.

Application of this Policy

This Policy sets out how Consortium handles the Personal Data of Consortium Personnel, Members, funders, suppliers, and all other third parties. We are a Data Controller under data protection law. This Policy applies to all Personal Data that we Process regardless of the media on which that data is stored and regardless of whether the person concerned has a current connection to Consortium.

The law requires Personal Data to be:

a) processed lawfully, fairly and in a transparent manner (see section: **Lawfulness, fairness and transparency**).
b) collected only for specified, explicit and legitimate purposes (see section: **Purpose Limitation**).
c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (see section: **Data Minimisation**).
d) accurate and where necessary kept up to date (see section: **Accuracy**).
e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (see section: **Storage Limitation**).
f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (see section: Security, Integrity and Confidentiality).
g) not transferred to another country without appropriate safeguards being in place (see section: **Transfer Limitation**)
h) made available to Data Subjects, and Data Subjects allowed to exercise, certain rights in relation to their Personal Data (see section: **Data Subjects' rights and requests**).

Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner. This means we have to tell? Data Subjects certain information about how we will use their Personal Data in a Privacy Notice (see below). In addition, we may only collect, process and share Personal Data fairly and lawfully and for specified purposes, some of which are set out below:

- the person has given their Consent (see **Consent**);
- the Processing is necessary for the performance of a contract with that person;
- to meet our legal compliance obligations;
- in some circumstances, to pursue our legitimate interests for purposes of helping us achieve our charitable aims.

These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly, legally and without adversely affecting the rights of Data Subjects. Our "Article 30 Record" helps us identify and document the legal ground being relied on for each Processing Activity.

Consent

A person consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be enough. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters. You will need to evidence Consent and keep records of all Consents so that Consortium can demonstrate compliance with Consent requirements. Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured (although exceptions may apply e.g. for safeguarding or other legal purposes). Consent may need to be refreshed if you intend to Process the Personal Data for a different and incompatible purpose which was not disclosed when the person first consented.

Privacy Notices

Data protection law requires us to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible,

easily accessible, and in clear and plain language so that a Data Subject can easily understand them. We have a standard Privacy Notice for these purposes, which may need to be adapted from time to time. Please contact the Responsible Officer if you have any questions about this.

This means that whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by data protection law, including the identity of the Data Controller and Responsible Officer, how and why we will use, Process, disclose, protect and retain that Personal Data, which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, if we use a recruitment agency or a Member provides us with personal information about its staff/volunteers), you must provide the Data Subject with all the information required by data protection law as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with data protection law, and on a basis which is consistent with how we will use the information.

Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary. For example:

- if someone signs up to our newsletter, we cannot use their email address for another reason.
- if we hold data on a current or past employee, we cannot share this in a reference to a prospective landlord or employer without their consent. The subject of the reference must notify Consortium if they wish us to provide such a reference.

Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. You may only Process Personal Data when performing your duties requires it. You cannot Process Personal Data for any reason unrelated to your duties.

Do not collect excessive data. Ensure any Personal Data you collect is relevant and adequate for the intended purposes. For example, when someone signs up for training with us you may ask certain questions for equal opportunities monitoring purposes, but not Personal Data that is unconnected to the training or our legitimate interests.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Organisation's Retention Policy.

Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which

we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

Consortium maintains retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time (see below). You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with the table below. This includes requiring third parties to delete such data where applicable.

Destroying personal data should be done is a secure way e.g. shredding of paper document, deleting the contents of a computer's recycle bin, and ensuring back-up hard drives or online systems also have the data deleted. You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Retention Policy

Key data processed by the Charity, and the timescale for retention are as follows (unless we are legally required to retain that information for a longer period):

Type of Personal Information	Period
Consortium Personnel	During the term of recruitment, office and for 7 years (or 5 years in the case of Trustees) following end of employment / office / appointment.
Applicants for voluntary and paid roles	During the recruitment process and for six months thereafter unless they become Consortium Personnel (see above).
Member Information – contact details for individuals at the member	During time with Member unless they request otherwise, and for six months thereafter.
Supplier Information – contact details for individuals at the supplier	During period of contract unless they request otherwise, and for six months thereafter.
Funder Information – contact details for individuals at the funder organisation	During period of contract unless they request otherwise, and for six months thereafter.
Survey Data	Psyeudoanonymised / anoynimised as soon as possible. In any event, identifiable Personal Data will be held no longer than 1 year.
Event webforms	1 month following the event unless consent obtained otherwise for specific data (e.g. for if the individual requests that their name is added to our mailing list)
Project webforms	For the duration of the project and 6 months afterwards, unless consent obtained otherwise for specific data (e.g. for if the individual requests that their name is added to our mailing list).
Mailing Lists	Only whilst active consent is given, renewed every 12 months.
Network Participant	During the time that individual is a participant in a network of Consortium and for 6 months thereafter.

Security, Integrity and Confidentiality

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data:

- **Confidentiality**: means that only people who have a need to know and are authorised to use the Personal Data can access it.
- **Integrity**: means that Personal Data is accurate and suitable for the purpose for which it is processed.
- **Availability**: means that authorised users are able to access the Personal Data when they need it for authorised purposes.

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. We will develop, use and maintain safeguards. This includes identifying risk and minimising these e.g. through encryption and Pseudonymisation where applicable. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect Personal Data.

You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure. For example, electronic devices must be password protected, so that if the device was stolen, the data could not be accessed. No Personal Data should be stored on memory sticks. Passwords should be used for online services such as email, and strong passwords should be used. Please speak to the Responsible Officer if you need further guidance on how to keep devices and online services secure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested. For example, if we partner with another organisation in a way where we may be sharing Personal Data, not only do we need to ensure that we have a legitimate basis to do so but we also need to ensure that the partner organisation has in place appropriate security measures to protect the Personal Data (see section: **Sharing Personal Data**). We should always have a written contract in place in such circumstances – please speak to the Responsible Officer.

Reporting a personal data breach

Data protection law requires us to notify Personal Data Breaches to the applicable regulator, and, in certain instances, the Data Subject. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Responsible Officer. You should preserve all evidence relating to the potential Personal Data Breach.

Transfer Limitation

Data protection law restricts data transfers to countries outside the European Economic Area in order to ensure that the level of data protection afforded to individuals is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country. This could include using a new online service where the servers are in the United States, for example. You must speak to the Responsible Officer before making any transfer outside the European Economic Area.

We can only transfer Personal Data outside the European Economic Area if one of the following conditions applies:

- the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPL. These will usually be clear in the terms and conditions e.g. of sites such as FaceBook, SurveyMonkey and Mailchimp who may be storing the data outside the European Economic Area;
- the Data Subject has provided explicit Consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in law.

Data Subjects' rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw Consent to Processing at any time;
- receive certain information about the Data Controller's Processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on automated processing;
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

We must verify the identity of an individual requesting data under any of the rights listed above (in particular, do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must acknowledge the request to the person requesting it, then immediately forward any Data

Subject request you receive to the Responsible Officer at dp@consortium.lgbt.

Accountability

Consortium must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. Consortium is responsible for, and must be able to demonstrate, compliance with the data protection principles. This means that Consortium must have adequate resources and controls in place to ensure and to document data protection law compliance including:

- identifying a data protection lead (this is the **Responsible Officer**);
- implementing 'Privacy by Design' (see **Privacy by Design and Impact Assessments**) when Processing Personal Data and using Impact Assessments where Processing presents a high risk to rights and freedoms of Data Subjects;
- integrating data protection into internal documents including this Policy, related policies, privacy guidelines and Privacy Notices;
- regularly training Consortium Personnel on data protection law requirements, this Policy, related policies, privacy guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis and Personal Data Breaches. Consortium maintains a record of training attendance by Consortium Personnel; and
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

Data protection law requires us to keep full and accurate records of all our data Processing activities.

Training and Audit

We are required to ensure all Consortium Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training. You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

Privacy by Design and Impact Assessments

We are required to implement 'Privacy by Design' measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles. You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

- what measures are available;
- the cost of implementation;
- the nature, scope, context and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Controllers must also conduct Impact Assessments in respect to high-risk Processing. You should conduct an Impact Assessment (and discuss your findings with the Responsible Officer) when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- automated processing;
- large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data.

An Impact Assessment must include:

- a description of the Processing, its purposes and the Controller's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

Direct marketing

We are subject to certain rules and privacy laws when marketing. For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email or text). The limited exception for existing customers known as 'soft opt-in' allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to (or similar transaction with) that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information. A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place. You may only share the Personal Data we hold with another employee, agent or representative of Consortium if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers, if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross-border transfer restrictions; and
- a fully executed written contract that contains certain approved third party clauses has been obtained (please speak to the Responsible Officer).

Key terms

Consortium: Consortium of Lesbian, Gay, Bisexual and Transgender Voluntary and Community Organisations, a company limited by guarantee registered in England and Wales with company 03534603.

Consent: agreement which must be freely given, specific, informed and be a clear indication of the wishes of the person we hold data on. The evidence of this is likely to be a statement or a clear positive action, showing agreement to the Processing of Personal Data relating to each person. See also section **Consent**.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. The Proud Trust is the Data Controller of all Personal Data relating to our Organisation Personnel and Personal Data used in our organisation. The Trustees and Leadership staff will lead on Data Control issues and processes.

Data Subject: a living, identified or identifiable individual that we hold the Personal Data of e.g. a contact at a Member. Data Subjects may be from the UK or residents of any country, and may have legal rights regarding their Personal Data.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Impact Assessment: tools and assessments used to identify and reduce risks of a data processing activity. Impact Assessments should be carried out at the planning stages of any major system or business change involving the Processing of Personal Data - which is called Privacy by Design. See also section **Privacy by Design and Impact Assessments**.

Personal Data: any information identifying a person or information relating to a person that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data, but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach. See also section **Reporting a personal data breach**.

Privacy Notices (also sometimes referred to as 'Fair Processing Notices'): separate notices setting out information that may be provided to people when Consortium collects information about them. See also section **Privacy Notices**.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept

separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions. Please remember that "Sensitive Personal Data" includes sexual orientation and Consortium considers that in certain cases gender identity may be Sensitive Personal Data, for example that someone is transgender.

Changes to this Data Protection Policy

We keep this Data Protection Policy under regular review. This Data Protection Policy does not override any applicable national data privacy laws and regulations in the United Kingdom.

Acknowledgement

All employees are required to acknowledge receipt of this policy, having read and understood its contents. This will be recorded on individual employee's records on Breathe HR system.