Confidentiality, Data Protection and Information Sharing Policy

1. Policy commitment

1.1 *Survive* recognises that confidentiality and securely managing personal and sensitive data are essential in building trust with clients and callers to our Helpline. *Survive's* Confidentiality, Data Protection and Information Sharing Policy sets out what confidentiality means within Survive, how we handle and store personal and sensitive data and when we might share personal and sensitive data.

1.2 The policy applies to all staff, sessional workers, and volunteers and continues to apply after their service or involvement with Survive has ended. See Appendix 1 for day-to-day implications and responsibilities.

1.3 *Survive* is required to collect, process and store personal data in relation to staff, trustees, volunteers and clients as well as funders and job applicants. Sometimes it may be necessary to share personal data with third parties, for example, where there is a safeguarding concern.

1.4 *Survive* is committed to adhering to the Data Protections Principles set out in the Data Protection Act 2018 (DPA) and with the UK General Data Protection Regulation (GDPR).

2. Legislation

2.1 The DPA states that an individual has the right to expect that personal information is protected, that it is fairly and lawfully obtained and processed and that it is not shared with third parties without the individual's consent. The DPA applies whether data is stored electronically, on paper or in any other format.

2.2 UK GDPR sets guidelines for the collection, processing, storage and sharing of personal data and sensitive personal data.

3. Definitions

3.1 Confidentiality

3.1.1 Anything a client or caller to our Helpline shares with *Survive* remains confidential within *Survive.* This means that staff and volunteers may discuss what they have been told with colleagues – for example during a meeting with their respective line managers, during a group supervision session or during a 1-1 supervision session.

3.1.2 On rare occasions it may be necessary to break confidentiality.
These occasions may broadly be defined as follows:

- a person is at risk of serious harm to themselves
- another individual is at risk of serious harm (e.g. the client or caller makes a specific threat to a named individual)
- a child is at risk of harm
- an adult is at risk of harm

(See also *Survive's* Suicide Policy, Safeguarding and Public Protection Policy – Adults at Risk and Safeguarding and Public Protection Policy – CYP)

3.1.2 When confidential information is shared without consent, the individual concerned must be informed and an explanation of the action given. Staff and volunteers must properly record the decisions that are made and the reasons for them.

3.2 Data
3.2.1 Data is information held on a computer including emails, images or voice recordings or on paper records that have been stored in a structured way so that information can be found easily.

3.2.2 **Personal data** is information which can directly or indirectly identify a person and includes name, email addresses (work and personal), addresses, bank details and medical information. UK GPDR categorises genetic and biometric data as personal data.

3.2.3 **Sensitive personal data** includes racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, physical or mental health conditions, trade union membership or non-membership, sexual orientation and criminal offences.

3.2.4 Note, victims and survivors of sexual offences are entitled to lifelong anonymity [Sexual Offences (Amendment) Act 1992] by prohibiting the publishing or broadcasting of their identity or information that might make their identity apparent, including their address or picture.

3.3 **Court orders**
From time to time, solicitors may request access to a client's records. We will not share any information with them until we are in receipt of a Court Order which should be addressed to the CEO. Once we are in receipt of a Court order, we are obliged to comply with it by law. We will inform the client (if they are not already aware of the request) and arrange for the client to read their records before we pass a copy of them to the solicitor or we will arrange to have the records read to them over the telephone. Note, we must supply a copy of the records in full – this means no redactions.

4. Data Protection Principles, *Survive's* commitment and practical application
4.1 The six principles that are central to the UK GDPR require that personal data must be:

GDPR principle	***Survive* commitment**	**Practical application (see also Appendix 1)**
Necessary for required service	•Obtain data for specific and lawful purpose. •Not process data in any manner incompatible with that purpose •Only request, collect and retain adequate and relevant data (i.e. not request more personal or sensitive data than is necessary)	•e.g. request contact details for GP but do not request medical records •Securely return any data sent to us in error or over and above our requirements
Processed fairly and lawfully and in a transparent manner	•Obtain and process data fairly and lawfully	•Clear procedure for consent including sharing of data with third party

in relation to the data subject	•Process in accordance with data subject's rights •Not pass on information to any person or agency outside Survive without the consent of the data subject or agency who provided it. •Not transfer data to any country that does not have equivalent levels of protection for personal data	contractors (e.g. Community Counselling) •Clear 'opt out' of mailings at any time •Remove any relevant personal or sensitive data received from a third party from a client's records (e.g. referral form), prior to the client viewing their records.
Used for clear and agreed purposes	•Collect data for specified, explicit and legitimate purposes •Only use information for the purpose for which it was given •Do not further process or share data in any manner incompatible with those purposes.	•Retain contact details for clients, funders, staff, volunteers or trustees •Retain contact details of client GPs in case of mental health or safeguarding concerns •Retain client notes as aide memoire for counselling /support work sessions
Kept for only as long as is necessary	•Not keep data for longer than is necessary. •Only retain information where there is a genuine organisational need to do so.	•Retain data for maximum of 7 years *(see Annual Data Audit at point 7*) after which all data will be securely destroyed – includes emails, paperwork, electronic files, funding applications, financial information. •Destroy client records 7 years after the last session.
Accurate and, when appropriate, kept up-to-date.	•Data to be accurate and kept up-to-date	•Maintain up-to-date contact lists •Correct errors
Processed securely and protected against unauthorised access, accidental loss, destruction, damage or deletion.	•Store data securely from unauthorised access, accidental loss, destruction, damage or deletion •Electronic data stored in a place of restricted access and/or password protected. • Hard copy data securely locked away. •Use appropriate technical measures to keep data secure	•Store personal or sensitive data securely and keep confidential conversations behind closed doors •Password protect electronic contact lists and mailchimp accounts and have different levels of access to different folders on Sharepoint •Not share data with third parties without consent or unless grounds to do so (e.g. safeguarding concerns).

		•Wherever possible, use numbers not names to identify clients •Store paper records in locked cabinets between use with the keys stored securely and archive paper records archived in locked cabinets in the lockable admin office •Mark documents containing personal or sensitive data 'Private and Confidential' •Lock phones and laptops when left unattended •Two-factor authentication for all email accounts; individual passwords and anti-virus software installed on laptops; use of secure servers

5. Data protection – the rights of individuals

Data protection right	**Meaning**	**Practical application (see Appendix 1)**
INFORMED	•Individuals informed how data is processed, shared, its purpose and how long it is retained.	•Induction consent form •Client consent form •Mailchimp opt out •Client-facing Confidentiality, Data Protection and Information Sharing Policy on website •Privacy policy on website •Secure explicit consent for use of anonymous and non-identifying quotes or case studies in reports, advertising, monitoring and funding applications
CHALLENGE	•Individuals can challenge the processing of data.	
CORRECTION	•Individuals can have inaccurate information corrected.	•Inform *Survive* administrator of any changes or corrections to personal data (e.g. changes to address, contact numbers) so that records can be updated •Maintain up-to-date contact lists
RESTRICT	•Individuals can restrict how data is used.	

DATA MOVEMENT	•Individuals can obtain or reuse personal data for their own purposes.	e.g clients can request a copy of their records to pass to a third party if it is there wish to do so and not due to coercion (see Appendix 1)
PROCESSING INFORMATION AND AUTOMATED DECISION MAKING	•Individuals know how data is used for automatic decision making, analysis or profiling.	•Client-facing Confidentiality, Data Protection and Information Sharing Policy on website •Privacy policy on website.
ACCESS	•Individuals are entitled to see what personal and sensitive data we hold and why, how it is used, stored and shared	•Staff, sessional workers and volunteers can access and change the personal data held about them on Breathe HR. •Enable clients to review their records with 5 working days notice •Process Data Subject Access Request Forms (see Appendix 2) • Remove any relevant personal or sensitive data received from a third party from a client's records (e.g. referral form), prior to the client viewing their records.
ERASURE	•Under the DPA individuals have limited rights to request personal data be erased (e.g. where processing causes unwarranted and substantial damage or distress). •Under UK GDPR, the right to be forgotten enables individuals to request the deletion or removal of personal data where there is no compelling reason for its continued processing.	Destroy data if data subject of that data requests it be removed from our records.

6. Data breaches
6.1 A data breach refers to the accidental or unlawful loss, destruction, damage or deletion or unauthorised disclosure of or access to data without the individual's permission.

6.2 Data breaches must be reported to the Information Commissioner Officers within **72 hour of the breach** being identified.

6.3 If a breach is suspected, the person who discovers or receives a report of the breach must **immediately** contact Survive's Data Protection Officer and complete a Data Breach Notification Form (see Appendix 3). If the breach occurs outside of normal working hours, the process must begin **as soon as is practicable.**

6.4 *Survive* has identified the CEO as its Data Protection officer who is responsible for day-to-day matters and any questions or concerns about the interpretation or operation of this policy.

6.5 *Survive* is the Data Controller under the DPA and is, therefore, ultimately responsible for implementation.

7. Annual data audit
7.1 *Survive* will conduct an annual data audit. This will involve a spot check of all data held electronically or in paper form and including all contact lists relating to clients, staff, volunteers, funders, media contacts, and 'friends' of *Survive*.

7.2 The annual data audit will review:
- how consent was gained for personal and sensitive data
- how data is stored
- how data is processed
- who has access to the data and how access is restricted
- how data protection policies and procedures have been shared with internal and external parties

7.3 The annual data audit will identify items which are more than 7 years old and require shredding.

7.4 The annual data audit will be conducted by the Operations Manager and Administrator who will highlight any actions taken to the CEO. The CEO will report the results of the annual data audit to the next Board of Trustees meeting.

8. Training
All staff, volunteers and trustees must complete GRPR training every three years.

Links to other policies
Confidentiality declaration
Privacy Policy – website
Client Consent Form
Safeguarding and Public Protection Policy – Adults at Risk
Safeguarding and Public Protection Policy – CYP
Suicide Policy
Disclosure Policy
APPENDIX 1

Your responsibilities

- Do comply with the Confidential, Data Protection and Information Sharing Policy
- Do ask questions if you are unsure about anything in the policy
- Do complete UK GDPR/Data Protection training every three years
- Do sign to state you have understood:
    - this policy and your role within it;
    - the Confidentiality Declaration as part of your contract;
    - the Safeguarding and Public Protection – Adults at Risk Policy
    - the Safeguarding and Public Protection – CYP Policy
- Do report data breaches – it is important that we all learn from errors to prevent recurrence in the future

Do's and don'ts of documentation

- Do ensure contact details for clients, staff, volunteers, funders, media contacts, and 'friends' of *Survive* are stored in Charity Log or in password protected files.
- Do immediately shred information which contains personal or sensitive data that is not to be kept including diaries, client records or post-it notes containing phone numbers
- Don't leave information that contains personal or sensitive data unattended – always place in a locked drawer when not in immediate use and lock everything away at the end of the day
- When working outside the office (satellite locations or home):
    - Do use the minimum possible documentation;
    - Don't include information that could identify a client (i.e. first names only, names should not be kept alongside addresses, or anything else that could identify a client)
    - Do store records in locked case or cabinet.
- Do use initials or first names only or client numbers to record appointments in diaries
- Do ensure there is no information contained in a personal diary that would link the information to *Survive*.
- Do not use information for any purpose other than that for which it was intended

Do's and don'ts of communication

- Do not request more information than is necessary (e.g. can request GP contact details but not medical records).
- Do update any changes to your personal details or those of your clients (e.g. addresses, phone numbers) on Breathe HR and/or Charitylog
- Don't discuss clients in public areas where likely to be overheard – keep confidential conversations behind closed doors
- When leaving messages regarding clients' appointments, do use first names only (never full names)
- Do use initials, appointment times or client numbers to identify clients whether on paper records, email, text, WhatsApp
- Do mark letters with personal or sensitive data 'PRIVATE AND CONFIDENTIAL'
- Do mark any personal or sensitive information sent by post as PRIVATE AND CONFIDENTIAL on outer and inner addressed envelopes and send via courier or recorded delivery
- Do write PRIVATE AND CONDIFENTIAL in the subject box when sending personal or sensitive information via email.
- Do double check addresses and email addresses before sending any personal or sensitive data

- Do secure explicit consent to use anonymized and non-identifying quotes ot case studies for reports, advertising, monitoring and fundraising applications.

Do's and don'ts of technology

- Do ensure phone and laptop are password protected
- Do lock screens on phones and laptops when leaving them unattended (e.g. tea break, toilet break, client appointment, etc).
- Do use Ctrl+Alt+Del to lock laptop screen.
- Do set laptop screen to auto-lock after 10 minutes of inactivity
- Do keep passwords safe

Do's and don'ts of office etiquette

- Don't allow clients into the admin office for any reason to protect any data which may be on view.
- Do lock the main office door when the admin office is unattended
- Do keep the key to the office with you at all times when in the building

Do's and don'ts of disclosure

- Do not disclose personal or sensitive data about *Survive, Survive* colleagues or clients other than to authorised persons in the course of the proper performance of your duties and with appropriate consent or permission
- Do check that third parties requesting personal or sensitive data are who they claim to be and that there is proper authorisation and/or consent from the data subject (i.e. written request sent from work email)
- Do pass on to the Counselling Manager, Support Services Manager, Supervisor or CEO, any requests for access to information under the Data Protection Act or UK GDPR from a data subject
- Do ensure that *Survive* is in receipt of a Court Order before releasing copies of client records to the courts or a solicitor. We must be in possession of a Court Order – even if it is the client who has requested access for their own solicitor or explicit and informed consent from the client/former client (see Disclosure Policy);
- Do inform clients if we have received a Court Order for access to their records and do give them the opportunity to read the records before we copy them (unredacted) for the courts
- Do ensure clients give permission before any information that is held about them by *Survive* is passed on to a third party where that information specifically identifies them or might lead to their identification.
- Do ensure any third party processor adopts appropriate technical and organisational security measures to safeguard personal and sensitive data in line with this policy (e.g. payroll).