WE ARE SURVIVORS.

Registered Office
Unit 9, Brewery Yard
Deva City Office Park
Salford
M3 7BB

+44 (0)161 236 2182
support@wearesurvivors.org.uk
wearesurvivors.org.uk

Twitter: @ThisIsSurvivors
Facebook: /ThisIsSurvivors
Insta: @thisissurvivors

Governance Policy

GDPR & Information Governance Policy

DOCUMENT CONTROL PANEL	
Title	**Title:** GDPR and Information Governance Policy **Version:** 003 **Reference Number:** WASIG2024
Supersedes	**Supersedes:** General Data Protection Policy, ICT Policy **Significant Changes:** Revised policy name and document control panel, merging of ICT Policy, inclusion of Records Retention & Destruction section, informational policy updates as part of review.
Originator or Modifier	**Originated by:** Hillyer McKeown LLP, Duncan Craig **Modified by:** Operations Director **Reference Material:** Directory of Social Change: Charity Policies and Procedures Templates (2023), ICO (https://ico.org.uk/for-organisations/), Data Protection Act (2018)
Ratification	**Referral Date:** 23.10.2023 **Referred by:** Operations Director **Ratified by:** Deputy Chief Executive Officer **Ratified Date:** 27.10.2023
Application	**Applies to:** All We Are Survivors Trustees, Employees and Volunteers **Authorised for inclusion in:** Quality Standards, Funding Application, Grant Agreements or Contracts, or other uses as agreed with Operations Director
Circulation	**Issue Date:** 24.01.2024 **Circulated by:** Operations Director **Accessible:** YouManage, Teams Drive (General > Files > Policies)
Review	**Last Review Date:** 05.02.2025 **Next Review Date:** 31.01.2026 **Reviewer Responsibility:** Operations Director

GDPR AND INFORMATION GOVERNANCE POLICY

1. Purpose and Scope

We Are Survivors takes the security and privacy of data seriously.

We need to gather and use information or 'data' about Trustees, staff, volunteers, clients, suppliers as part of our business and to manage our relationship with all these parties.

We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the UK General Data Protection Regulation ('UK GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

This policy applies to current and former employees, volunteers (including Trustees), apprentices and consultants. It also applies to those that have used our services (7 years post last contact) and those engaged in or have been referred to us.

Anyone that falls into one of those categories is the 'data subject' for the purposes of this policy.

Employees should read this policy alongside their contract of employment and any other notice we issue to you from time to time in relation to your data.

We Are Survivors has measures in place to protect the security of all data.

We Are Survivors will hold data in accordance with our statutory data protection and retention obligations as may be required by law. We will only hold data for as long as necessary for the purposes for which we collected it, and in line with our Employee Privacy Notice, and 'Client Contract'.

We Are Survivors is a 'data controller' for the purposes of the personal data. This means that we determine the purpose and means of the processing of your personal data.

This policy explains how We Are Survivors will hold and process individuals' information. It explains individuals' rights as a data subject. It also explains staff obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

For all employees, this policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by We Are Survivors at any time. It is intended that this policy is fully compliant with the 2018 Act and UK GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and UK GDPR.

2. What is Covered by This Policy?

This policy covers data protection in relation to all areas of We Are Survivors activities, including:

- customer records.
- legal compliance (UK General Data Protection Regulation – UK GDPR).
- recruitment, promotion, training, redeployment and/or career development.
- administration and payment of wages.
- calculation of certain benefits, including pension.
- disciplinary purposes arising from an employee's conduct or inability to perform their duties.

- performance review.
- recording of communication with employees and their representatives.
- compliance with policy and/or legislation regarding health and safety or other employment legislation and regulation.
- provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future employers.

3. General Data Protection and the Internet

The internet as a resource is constantly changing. These guidelines will be updated in the light of experience and developments of the internet itself.

You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that we have accessed the page or file via company devices of systems, might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

We may block or restrict access to some websites at our discretion.

a. Acceptable Uses

As a general principle, internet access, via any piece of technology provided by We Are Survivors or using We Are Survivors internet connections, is provided to employees, workers, volunteers, apprentices, and consultants to support work related activities. The following list is not intended to be a definitive list, but sets out broad areas of use that the organisation considers to be acceptable uses of the internet:

- to provide communication within the organisation via email or the organisation website.
- to provide communication with other organisations for educational purposes.
- to distribute electronic copies of the newsletter, monthly community development activities calendar or informational documents, as authorised by the Chief Executive Officer.
- to distribute details regarding organisation meetings.
- to provide electronic methods of communication.
- any other use that directly supports work related functions.

b. Unacceptable Uses

The following uses will be regarded as not acceptable:

- using the computer to perpetrate any form of fraud, or software, film or music, including spoken word, piracy.
- use for racial, sexual, homophobic or other harassment.
- use of non-educational games.
- to access pornographic and adult content (unless approved by the Deputy Chief Executive Officer or Director for use in developing client engagement, e.g. sex/cruising apps), obscene or illegal material.

- to solicit personal information with the intent of using such information to cause harm.
- entering into a commitment on behalf of the organisation (unless you have explicit permission to do this from the Deputy Chief Executive Officer on in absence the Chief Executive Officer).
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- hacking into unauthorised areas.
- publishing defamatory and/or knowingly false material about the organisation, your colleagues and/or our clients on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
- revealing confidential information about the organisation in a personal online posting, upload or transmission – including financial information and information relating to our clients, staff and/or internal discussions.
- undertaking deliberate activities that waste staff effort or networked resources.
- introducing any form of malicious software into the organisation network.
- to disrupt the work of other users – this includes the propagation of computer viruses and use of the internet.
- use of any Bit torrent systems.
- use for personal or private business purposes, unless permission granted by a Director.

c. Netiquette

The following general principles should be adopted:

- be polite.
- do not be abusive in messages to others.
- use appropriate language.
- remember that you are a representative of the organisation and that you are using a non-private network.

4. General Data Protection and Social Networking Sites

Social media applies to blogs, microblogs like, videos, social network platforms, discussion forums, ‘wikis’, and other personal webspace. We Are Survivors permits the use of internet and social media on work premises, outside of normal working hours ((that is, during your lunch break, and before or after work (whilst you are still on organisational premises), but only where it meets the following guidelines:

- this is usually outside normal working hours and must not interfere with your or others day-to-day duties.
- personal access should not be in view of any clients, and you are reminded to log out or lock your device immediately upon leaving your mobile phone or PC, even if only for a short period.

- do not "speak" for the organisation unless you have express permission to do so by the Chief Executive Officer, this covers all comments relating to the organisation.
- protect yourself from identity theft.
- if you can be linked to the organisation, act appropriately. This includes photos and status updates.
- remember that colleagues, prospective employers, parents and children may see your online information.
- if in doubt, please seek advice from your Line Manager.

5. Data Protection Principles

Personal data must be processed in accordance with the six 'Data Protection Principles'. It must:

- be processed fairly, lawfully and transparently.
- be collected and processed only for specified, explicit and legitimate purposes.
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed.
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay.
- not be kept for longer than is necessary for the purposes for which it is processed and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

6. How We Define Personal Data

'Personal data' means information which relates to a living or deceased person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination.

For Employees and Volunteers (including Trustees)

We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments.
- your contact details and date of birth.
- the contact details for your emergency contacts.

- your gender.
- your marital status and family details.
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement.
- your bank details and information in relation to your tax status including your national insurance number.
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us.
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings).
- information relating to your performance and behaviour at work.
- training records.
- electronic information in relation to your use of IT systems/swipe cards/telephone systems.
- your images (whether captured on CCTV, by photograph or video) and
- any other category of personal data which we may notify you of from time to time.

For Clients

We will collect and use the following types of personal data about you:

- referral information completed by you or the referrer.
- the contact details for your emergency contacts.
- your contact details (including address).
- your date of birth.
- your gender and gender assignment.
- your marital status and family details.
- your employment status.
- your GP contact details and appropriate medical information (including medication or any other information that would support our effort to safeguard you).
- details on the purpose of your referral (including sensitive data relating to the crime/incident committed against you).
- details of engagement with Criminal Justice Services (including contact details of police).
- details created by us on the answers you provide during assessment (risk, wellbeing) and
- any other category of personal data which we may notify you of from time to time.

7. How We Define Special Categories of Personal Data

'Special categories of personal data' are types of personal data consisting of information as to:

- your racial or ethnic origin.
- your political opinions.
- your religious or philosophical beliefs.
- your trade union membership.

- your genetic or biometric data.
- your health.
- your sexual orientation and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

8. How We Define Processing

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage.
- adaption or alteration.
- retrieval, consultation or use.
- disclosure by transmission, dissemination or otherwise making available.
- alignment or combination and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

9. How Will We Process Your Personal Data?

The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

Recruitment and Selection

If placing a recruitment advert, We Are Survivors must identify itself properly – people should know who they are applying to. If using a recruitment agency, We Are Survivors must ensure the agency identifies itself.

Information collected for recruitment or selection for an interview must be used for that purpose only and must be kept securely. Where sensitive personal data is collected, explicit written consent should be obtained from applicants at the point of data collection. The Operations Director should ensure that equal opportunities data for applicants is anonymised before the applications are considered.

If verifying the information a person provides, We Are Survivors must ensure the person knows how this will be done and what information will be checked.

If We Are Survivors needs to verify criminal conviction information, it will only do this by getting a Disclosure and Barring Service (DBS) check. We Are Survivors must ensure it is entitled to receive this information and must follow the DBS's procedures strictly. We Are Survivors may only keep a record that a satisfactory/unsatisfactory check was made, but it may not store any detailed information.

Employment Records

We Are Survivors is permitted to collect, maintain, and use employment records. However, staff should know what information about them is kept and what it will be used for. We Are Survivors will not keep information for which it has no genuine business need or legal duty to keep.

Employment records must be kept in a secure, locked place, and computerised records must be password protected. Only authorised staff should have access to employment records (usually, the individual's Line Manager, relevant Director, HR Manager, and the Deputy/Chief Executive).

We Are Survivors will keep employment records of staff who have left for three years to allow for information to be supplied for references. After this time, records will be destroyed.

Sickness Records

We Are Survivors will collect information about a staff member's health in accordance with We Are Survivors Sickness Policy and Procedure and record it on YouManage. Access to the information is strictly limited to authorised staff.

Pension or Insurance Scheme Records

We Are Survivors will only use the information about a staff member for the administration of the scheme and will inform the staff member of what information the insurance company or scheme provider will pass back to We Are Survivors.

Disclosure

We Are Survivors will only disclose information on a staff member if, in all the circumstances, it is satisfied that it is in line with UK GDPR and is reasonable to do so or as part of legal disclosure. Fairness to the staff member will always be We Are Survivors first consideration. We Are Survivors will allow staff access to their own records to ensure the information is correct.

We Are Survivors Staff Rights

Staff have a legal right of access to the information We Are Survivors holds on them and the right to challenge the information if it is thought to be inaccurate or misleading. If a staff member objects to We Are Survivors holding or using information about them because it causes them distress or harm, We Are Survivors will delete the information or stop using it in the way complained about unless We Are Survivors has a compelling reason to continue holding and/or using that information.

To see what information, We Are Survivors holds on you, ask the Deputy Chief Executive Officer for access to your records.

Customer Data

We Are Survivors will process personal data that may identify a client or prospective client according to UK GDPR.

Client data will be processed in the legitimate interest of We Are Survivors work and/or if We Are Survivors has a contractual or legal obligation. Such data will be retained for 7 years from the date of the last contact with the organisation.

Processing

We will use employee's personal data for:

- performing the contract of employment (or services) between us.
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing.

We may be required to collect and process data relating to criminal convictions of employees, workers, volunteers and other individuals engaged with We Are Survivors. Further information can be found in our Privacy Notice, which can be obtained from the Information Governance Lead.

We might process special categories of your personal data for the purposes listed above which have an asterisk beside them. We will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members

We do not take automated decisions about you using your personal data or use profiling in relation to you at any point.

We will only process special categories of your personal data in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data, then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the Information Governance Lead.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law.
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent.
- where you have made the data public.
- where processing is necessary for the establishment, exercise, or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

We will use client's personal data for:

- designing, developing and delivering care and treatment plans.
- delivering services.
- complying with any legal obligation.

We can process personal data for these purposes without the individual's knowledge or consent. We will not use any personal data for an unrelated purpose without telling individual about it and the legal basis that we intend to rely on for processing it.

If individuals choose not to provide us with certain personal data, they should be aware that we may not be able to carry out certain parts of the contract between us.

For example, if employees do not provide us with their bank account details, we may not be able to pay them. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

If a client does not provide us with contact details, we may not be able to provide services to them as we're unable to be in contact.

10. Sharing Your Personal Data

Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

The following companies carry out legitimate activities on behalf of We Are Survivors:

a) Finance Manager and Payroll Bureau.
b) HR Manager.
c) Williamson Croft (Accountants).
d) ARO (Telephony & Connectivity Systems).
e) Yellowgrid (IT Systems).
f) iTech Managed Services (Printing Solutions).

We may store data in the UK or the European Economic Area, or any country deemed to be adequate by either the UK or the EU. Where We Are Survivors stores data outside these jurisdictions, it may undertake a data transfer risk assessment. You will be notified of the transferring and the protections which are in place to protect the security of your data. The Company will ensure appropriate UK safeguards are in place to protect the rights of those identified by personal data stored in such locations.

11. How Should You Process Personal Data for the Company?

Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored, and handled appropriately, in line with this policy.

The Company's Information Governance Lead is responsible for reviewing this policy and updating all employees, volunteers and contractors on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

You should **never** disclose the personal data of any employee, worker, volunteer, consultant, contractor, service user or client of We Are Survivors (or any of the organisation's contacts or any associated individuals) unless you have been explicitly instructed to do so or are expressly required to do so.

You should not share the personal data of any employee, worker, volunteer, consultant, contractor, service user or client of We Are Survivors informally.

You should keep personal data secure and not share it with unauthorised people.

You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

You should not make unnecessary copies of personal data and should keep and dispose of any copies securely, particularly any special category personal data as defined above, which includes the personal data and records of clients and service users, employees, workers, volunteers, apprentices, and consultants.

12. Data Sharing

We Are Survivors at times will need to share individuals' data for us to fulfil our obligations in delivering services, supporting clients, employing, and managing staff, and hosting and engaging volunteers.

If the organisation enters in to a partnership or similar with another agency/agencies, a DPIA (Data Protection Information Assessment) to assess if an ISA (Information Sharing Agreement) is required.

The Operations Director will take responsibility for fulfilling this requirement of our Information Governance obligations.

Information on any individual should not be shared outside of the organisation without their expressed permission, unless for the purposes of safeguarding individuals.

For data pertaining to clients, information should only be shared with those individuals or agencies that expressed permission has been obtained and recorded in VIEWS. Clients have the right to be anonymous within the organisation and staff should do everything to protect an individual's anonymity.

The safeguarding directly of an individual (client or other) or the identification that a child, young person, or vulnerable adult is at risk, may require the sharing of appropriate personal data of any

individual without their permission, which the organisation encourages with caution as part of our safeguarding commitment.

The Safeguarding Lead should be counsel for anyone wishing to break confidentiality and share data without permission.

13. Systems & Data Security

The Company has robust systems in place to protect its data, both on and offline. All employees, workers, volunteers, apprentices, and consultants have a responsibility to be alert to security risks and report anything that is of concern about to the Information Governance Lead.

Data should only be accessed via devices and systems that have been provided by We Are Survivors, with the exception of Breathe HR which may be accessed on a personal device. Each device and system will be passcode / password protected with a strong password, and in some instance, have additional multi-factor authentication requirements. Passwords will be changed on a regular basis, with systems requesting a change, roughly, every 90 days.

You must only log on to our systems using your own username and password. You must not use another staff members username and password or allow anyone else to log on using your username and password. The Operations Director or Deputy Chief Executive Officer, with reasonable explanation, may access systems using your username and password, or may grant permission for a member of Operations staff or Yellowgrid to do so. Usually, in these situations, it will be to fix or support the fixing of a system.

We permit the incidental use of our systems to send personal emails, browse the internet and make personal telephone calls subject to certain conditions. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

Personal use must meet the following conditions:

- it must be minimal and take place exclusively outside of normal working hours
- personal emails should be labelled "personal" in the subject header
- it must not affect your work or interfere with the business
- it must not commit us to any marginal costs
- it must comply with our policies including the Equal Opportunities Policy, People Conduct Policy, GDPR & IG Policy and Disciplinary Procedures

We Are Survivors' devices are installed with Trend and Microsoft Defender anti-virus software.

You should lock your computer screens when not at your desk and at the end of your working day, any device must be switched off to help ensure that the anti-virus software is regularly updated as required.

With any device, you should not use the device to store We Are Survivors' work on the desktop – it must be saved within the appropriate folder on OneDrive.

All devices will be provided on the first day of an individual's induction, if a device is required to be shipped – this will be tracked by the Operations Director via the shipping company (usually DPD). Once a device has been provided to an employee, worker, volunteer, apprentice, and consultant, it is their responsibility for the reporting of any device defects or lost equipment. In the event equipment has been lost, you must inform the Operations Director as soon as you believe the device is lost. The Operations Director will then lock the device via Microsoft Azure admin panel.

Do not save personal data to your own personal computers or other devices, whether it be the personal data of employees, workers, volunteers or clients and service users.

Personal data should be sent via Criminal Justice Secure Mail (CJSM), especially with regards to clients or service users. If discussing client cases via Outlook, all data must be anonymised using a client or service users Unique Reference Number (URN) or using separate keys/codes so that the data subject cannot be identified. Other personal data should be encrypted before being transferred electronically to authorised external contacts (where possible), including using zip folders and secure means of transferring data.

We monitor all e-mails passing through our system for viruses. You should exercise caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments, or click any links in it.

The following general principles should be adopted about emails:

- Whenever e-mail is sent, it should be from an official work email address which includes the sender's name, job title and organisation's name as minimum signature.
- Staff must use the internal contacts list via central@wearesurvivors.org.uk and before sending an email, must check that the address is the most up to date by cross-checking across CRM systems.
- Ensuring that we have consent to email when contacting a client through this format.
- Take note of the external indicator function when emailing outside the organisation.
- Use encryption function or secure email when sending any information which identifies information of a client.
- Every user is responsible for all mail originating from their user ID (e-mail address).
- Forgery or attempted forgery of electronic mail is prohibited.
- Attempts to read, delete, copy or modify the e-mail of other users is prohibited.
- Attempts to send junk mail and chain letters is prohibited.

If you receive e-mail from outside the organisation that you consider to be offensive or harassing, speak to your Line Manager.

Harassing internal e-mails will be dealt with under the organisation's guidelines.

You should be aware that, in the event of the organisation being involved in legal proceedings, any relevant e-mails (including internal e-mail) may have to be disclosed, on the same basis as is the case for written documents.

Email should be accessed via organisation provided equipment only, if you wish to use a personal device to download organisation emails, you must check with your line manager first

You will need to ensure that your device is always secured by a password, that this password is not shared with any other person and that all reasonable care is taken to prevent unauthorised access to confidential information.

Inform the Operations Director immediately, or in their absence the Deputy Chief Executive Officer, if you suspect your computer may have a virus.

Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications.

For business reasons, and to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.

We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

- to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy
- to find lost messages or to retrieve messages lost due to computer failure
- to assist in the investigation of alleged wrongdoing
- to comply with any legal obligation

Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer.

You should lock drawers and filing cabinets, especially when you leave the office or are away from your desk for a prolonged period. Do not leave paper with personal data lying about, for example on printers or on your desk, particularly if you are away from your desk for a prolonged period.

You should not take personal data away from Company's premises without authorisation from your line manager or Information Governance Lead.

Personal data should be shredded (via a Cross-Cut Shredder) and disposed of securely when you have finished with it.

You should ask for help from our Information Governance Lead if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

14. How to Deal with Data Breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact the Information Governance Lead immediately and keep any evidence, you have in relation to the breach.

15. Subject Access Requests

Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to the Information Governance Lead who will coordinate a response.

If you would like to make a SAR in relation to your own personal data, you should make this in writing to Information Governance Lead. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond to your request.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request. This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

16. Your Data Subject Rights

You have the right to information about what personal data we process, how and on what basis as set out in this policy.

You have the right to access your own personal data by way of a subject access request (see above).

You can correct any inaccuracies in your personal data. To do so, you should contact the Information Governance Lead.

You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

You have the right to object if we process your personal data for the purposes of direct marketing.

You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

With some exceptions, you have the right not to be subjected to automated decision-making.

You have the right to be notified of a data security breach concerning your personal data.

In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Information Governance Lead.

In following Article 17 of the UK GDPR, the company allows all individuals the right to have any personal information that we hold, erased (also known as 'right to be forgotten'). In this instance the company will only erase the records that it currently holds, any records created in the future – the

right will not apply. Anybody can apply their right to erasure and the destruction of all personal records will be destroyed when:

- The personal data is no longer being used for the purpose it was collected or processed.
- Consent in holding the personal records is withdrawn.
- There is a required legal obligation.
- An individual objects to the processing of their data and there is no overriding legitimate interest to continue this processing.
- Personal records have been processed unlawfully

An individual can make a request for erasure, with verbally or in writing to the Information Governance Lead, who will have 1-month from the receipt of the request to either erase all requested data or decline any request. Providing confirmation or reasoning for either outcome. The Information Governance Lead has the right to request further identification checks before any request is processed.

While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Information Governance Lead.

The company has the right to refuse the right to erasure when a request is distinctly unfounded; overlaps with other requests or is a repeat of a previously made request. Where this applies the company will be expected to explain why they have refused this right, and, if asked, explaining the refusal to the Information Commissioner's Office.

You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

17. Records Retention & Destruction

The company strictly follows UK GDPR requirements to destroy records that are no longer needed for the purpose in which they were collected (Article 5 1(e)) and complies with documentation requirements by setting standard retention periods, as outlined below.

All client records will be stored and maintained for 7 years, after which all records will be destroyed (as set out in the 'Your Data' leaflet each client receives). As such, the company have a Client Records Retention & Destruction Schedule (see: Appendix 1) in place:

- Each quarter end, under the direction of the Information Governance Lead, the Senior Operations: Data Analyst will export a report from our Views CMS that will return all clients that have been *'Inactive' for 7 years.
- Those identified in the report, will have all records deleted including:
    - Digital files from the clients OneDrive folder
    - Digital records held on Views
    - Digital contact card held on Outlook

- First name and Surname held on digital URN Generator

The Information Governance Lead will hold all responsibility for the appropriate destruction of all client records, they will make record of:

- Person ID (Views)
- URN
- Forename
- Surname
- Last Referral Date
- Last Session/Contact Date
- File(s) Destroyed?
- File(s) Destruction Date
- Authorising Staff Member

*The company defines 'Inactive' as from the date of the of the last entry of any activity in the client record.

All employees, workers, volunteers, apprentices, and consultants' records will be stored for 6 years, after which all records will be destroyed - unless there is necessary company reason for not doing so. The Information Governance Lead holds a register of each employee who has left the company in the last 6 years, ensuring all employment contracts and other records relating to individuals' employment with the company are destroyed on the 6-year anniversary.

To safeguard the company against any legal claim where an applicant for a role within the organisation has been rejected, the company will keep all records including application; shortlisting comments and interview questions and notes on record for 6 months before destruction.

Where the company has enacted the destruction of any of its stored records, where applicable all data will be removed from its back-up data storage system Afi (https://afi.ai/).

18. Summary for Staff

We Are Survivors employees should bear in mind the following considerations:

- Sensitive and confidential information must be treated with particular attention.
- Personal data must not be emailed to staff members' personal email accounts, as there is no guarantee of security of these accounts.
- Any personal data stored in paper format must be held securely locked in filing cupboards in We Are Survivors office. If it has to leave the office, consider pseudonymisation.
- All We Are Survivors personal computers must be password protected. All personal data should be kept in the appropriate IT system (i.e. customer details in [relevant CRM system] and staff details in [HR management system]). If electronic equipment is lost or stolen, access to the server and database from that piece of equipment will be severed.
- The database holding customers' personal data must be accessed only via We Are Survivors electronic equipment. All employees and volunteers will be trained on how to use the

database relying on the written procedures for entering, amending and maintaining data. These procedures will be reviewed annually.

- In line with We Are Survivors IT Security Policy, no personal data (or other files) should be stored on [charity's name]'s electronic equipment. If you download any files for ease of working, make sure you save them in the appropriate place on [location], password protected, if necessary, as soon as you have finished working on them and delete any local files.
- Any changes to personal data (e.g. a change in home address) must be updated on the [relevant CRM system] database within 28 days of receipt.
- Personal data must not be given out to any third party unless the individual has agreed to release this information.
- Any personal data kept in paper format that is no longer required must be destroyed.
- Any personal data kept electronically that is no longer required must be deleted.
- We Are Survivors will carry out data minimisation as part of the annual data audit.
- If data needs to be processed for profiling or for other statistical information, pseudonymise it. The procedures for this should be documented to ensure that the identification of the individuals is kept separate from the processed data.

WE ARE SURVIVORS.

Appendix 1

Client Records Retention & Destruction Map