Sufra NW London

Data Protection Policy

Policy Owner:	Deputy Director	To be approved by:	Board of Trustees
Last reviewed by policy owner on:	23/05/2025	Approved on:	04/06/2025
Next Review Date:	May 2027	Review frequency:	Every 2 years

1 Introduction

Sufra NW London is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all our legal obligations.

We hold personal data about our employees, service users, volunteers, suppliers, business contacts, and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the charity's data protection standards – and to comply with the law.

1.1 Purpose

Sufra NW London needs to keep certain information on its employees, volunteers, service users, and trustees to carry out its day-to-day operations, to meet its objectives, and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt in line with the UK GDPR (General Data Protection Regulation) and the Data Protection Act 2018. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

1.2 Scope

This policy applies to:

- The head office of Sufra NW London
- All branches or points of delivery
- All staff and volunteers of Sufra NW London
- All contractors, suppliers and other people working on behalf of Sufra NW London

It is important to stress that Data Protection Legislation applies to everyone handling personal data on behalf of the charity.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy with additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

It applies to all data that the charity holds relating to identifiable individuals, even if that information technically falls outside the scope of the data protection law. This can include:

- Names of individuals
- Postal addresses
- Telephone numbers

Special categories of personal data we may hold include:

- Race/ ethnic origin
- Religion
- Biometrics (where used for ID purposes)
- Health data
- History of criminal convictions

1.3 Why this policy exists

This Data Protection Policy ensures that Sufra NW London:

- Complies with data protection law and follows good practice
- Protects the right of staff, service users and partners

- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

1.4 Definitions

1.4.1 PERSONAL DATA

Personal data means information relating to an identified or identifiable individual. This might be anyone, including a customer, client, employee, partner, member, supporter, business contact, public official or member of the public. It does not need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data. 'Data' includes that based on paper as well as that kept on computer.

1.4.2 DATA PROCESSOR

The processor or data processor is a person or organisation who deals with personal data as instructed by a controller for specific purposes and services that involve personal data processing - for example our referral partners.

1.4.3 DATA CONTROLLER

A data controller is a person, company, or other body that determines the purpose and means of personal data processing (this can be determined alone, or jointly with another person/company/body) - Sufra NW London is a data controller.

1.4.4 PROCESSING

The definition of 'processing' is obtaining, using, holding, amending, disclosing, destroying, and deleting personal data.

1.5 Data protection law and guidelines

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018. It sits alongside the UK GDPR.

General Data Protection Regulation sets out the key principles, rights and obligations for most processing of personal data, describing how organisations including Sufra NW London must collect, handle, and store personal information. These rules apply regardless of whether data is stored electronically, on paper, or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely, and not disclosed unlawfully.

1.5.1 LAWFUL BASIS FOR PROCESSING DATA

We must ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose, the period of which it will be retained and the data subjects' rights. This should occur via a privacy notice on all forms requiring the collection of this data as well as our website. This applies whether we have collected the data directly from the individual, or from another source.

It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply the lawful basis. At least one of the following conditions must apply whenever we process personal data:

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose. For instance, this may include Volunteer Application Forms where consent is recorded via the applicants' signature on the form which includes our privacy statement. When we are capturing data on the basis of consent, we will monitor and refresh consent as appropriate. Consent should be informed, specific and given freely. Sufra NW London respects an individual's right to withdraw consent. When processing data on the basis of consent, we will keep records that demonstrate the following:
    - Who consented
    - When they consented
    - What they were told at the time of consent
    - How they consented
    - Whether they have withdrawn consent
- **Contract:** the processing is necessary to fulfil or prepare a contract for the individual.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests:** processing the data is necessary to protect a person's life or in a medical situation.
- **Public function:** processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
- **Legitimate interest:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect

the individual's personal data which overrides those legitimate interests. This basis is applied to our collection of beneficiary data such as Food Bank, volunteering and Community Kitchen guests. Where Legitimate Interest is the basis for processing data, staff should always consider the purpose of collecting data, the necessity of the data to achieve the purpose, risks of holding the data and mitigations (eg training, using secure platforms, access to privacy notices, data anonymising) in place and the implications on an the individual who data is being collected on (eg on their privacy). See Appendix B.

1.5.2 PRINCIPLES

Sufra NW London is committed to following the six Principles of Data Protection set out in the General Data Protection Regulations (GDPR). Any personal information that you share with us will be:

- processed lawfully, fairly and in a transparent manner.
- collected for specified purposes which we explain to you.
- necessary to achieve our stated purpose. We will not collect personal information that is not essential to our purpose.
- kept as accurate as possible and, where necessary, kept up to date.
- kept for no longer than is necessary.
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

2 Risks and responsibilities

The Data Protection Officer (DPO) at Sufra NW London is Gill Carter, Deputy Director. All data protection concerns should be shared with your line manager and then with the DPO.

2.1 Data protection risks

This policy helps to protect Sufra NW London from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.

- **Failing to offer choice**. For instance, all individuals should be free to choose how the charity uses data relating to them.
- **Reputational damage**. For instance, the charity could suffer if hackers successfully gained access to sensitive data.

2.2 Responsibilities

Everyone who works for or with Sufra NW London has some responsibilities for ensuring data is collected, stored, destroyed and handled appropriately.

Each person that handles personal data must ensure it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The **Board of Trustees** is ultimately responsible for ensuring that Sufra NW London meets its legal obligations.

Sufra NW London employees are responsible for:

- Keeping data secure by using strong passwords, not sharing data with unauthorised personnel and never saving personal data on unsecure/personal devices.
- Ensure data is only shared using secure methods (eg password protected files) and to authorised personnel.
- Attending and engaging in Data Protection Training.
- Reporting any data breaches and implementing follow up actions.
- Completing a Data Protection Impact Assessment (DPIA) before any new activity that could pose a high risk to individuals' rights, such as large-scale processing of sensitive data, use of CCTV, profiling, or working with vulnerable groups. DPIAs must be reviewed and approved by the DPO. See Appendix A.
- Keeping data up to date and accurate.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Ensuring our case management process upholds confidentiality in line with our confidentiality policy.
- Performing regular checks and scans to ensure security hardware and software is functioning properly. For instance, cloud computing services.
- Addressing any data protection queries and subject access requests.

- Where necessary, working with other staff and volunteers to ensure that the organisation abides by data protection principles, i.e. abiding by data retention schedules to ensure data is disposed of, archived or anonymised.

2.3 General staff guidelines

- Do not open suspicious emails, links, or attachments
- The only people able to access data covered by this policy are Sufra NW London employees and specific volunteers with a valid DBS check and who have received training. Specific volunteers include those assisting the Organisation with data entry and administration, or those delivering a service, for instance counselling or advice work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager if they are unsure about any aspect of data protection.
- **Avoid public or unsecured Wi-Fi** connections for work-related tasks
- Limit administrative privileges to only those who need them

2.4 Data storage guidelines

These rules describe how and where data should be safely stored. Please refer to our Personal Data Inventory to find a detailed description as to which data we store and why. It is important for all employees of Sufra NW London to be clear about the various types of data we collect.

These guidelines also apply to data that is usually stored electronically but has been **printed out** for some reason:

- In cases when data is stored on paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- When not required, the paper or files should be kept in a locked drawer or filling cabinet
- Employees and authorised volunteers should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and should never be shared between employees.
- If data is stored on removable media (like on a memory stick, CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the charity's standard backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- All servers and computers containing data should be protected by approved security software and a firewall.

2.5 Data use guidelines

Personal data is of no value to Sufra NW London unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when let unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

2.6 Guidelines for data accuracy

The law requires Sufra NW London to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Sufra NW London should put into ensuring its accuracy.

It is the responsibility of all work employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a volunteer's details from time to time.
- Data should be updated as inaccuracies are discovered. For instance, if a volunteer can no longer be reached on their stored telephone number, it should be removed from the database.

2.7 Guidelines for data retention

Sufra NW London keeps documents under the following headings:

- Governance
- Finance
- Staff management
- Monitoring and evaluation
- Client case records
- Health and Safety
- Administration
- Building and utilities
- External agencies

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained.

All trustees and staff members have a responsibility to manage the charity's record keeping using the following retention schedule.

Type of document	**Retention period**
Governance	6 years

Finance	Permanent
Staff Management (including consultants)	6 years
Volunteers	3 years after termination
Client case records	6 years
Newsletter recipients	Until unsubscribed
All other types	1 year

2.8 Guidelines for destroying data

Data which is no longer in use should be destroyed in a safe and secure manner. The Personal Data Inventory indicates how long each type of data will be retained.

After its' retention period, staff must ensure that the data has been deleted from where it is stored online (e.g. OneDrive folders) or electronically (e.g. computerised folders and recycle bin, mobile phones), and that data stored on paper has been shredded. Care should be taken to ensure destruction does not compromise client confidentiality (for example, by using a shredder).

Once data retention periods have passed, we will attempt to permanently delete data to the best of our ability, so this data is beyond use. We will make efforts to delete data from our systems. Any data that remains on our systems, we are committed to:

- not using the personal data to inform any decision in respect of any individual
- not giving any other organisation access to the personal data;
- applying appropriate technical and organisational security where needed
- permanently deleting the information if, or when, this becomes possible.

In certain instances when data may need to be stored past its retention period, such as for monitoring and evaluation purposes, it will need to be anonymised. This can be done using Sufra NW London's electronic case management system, Advice Pro.

For all case files stored on Advice Pro, a request will be submitted at the beginning of each year to Technical Support by the Programmes Manager for all cases that have reached the end of their retention period to be archived. Archived case files will not be accessible to Case Workers, except for basic demographic details for the purpose of statistical analysis.

2.9 Guidelines for data sharing

By 'data sharing' we mean the disclosure of data from one or more organisations to a third-party organisation or organisations, or the sharing of data between different parts of an organisation. Data sharing typically involves personal data being disclosed

between a number of organisations, all of whom have a responsibility to comply with the DPA, including its fairness provisions.

As part of the process and to ensure best practice, a data sharing agreement should be put in place, setting out what information will be shared, how it will be shared and the security measures put in place to protect it.

Data Sharing can take two main forms:

- Systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose.
- Exceptional, one-off decisions to share data for any of a range of purposes.

Data sharing can take the form of:

- A reciprocal exchange of data.
- One or more organisations providing data to a third party or parties.
- Several organisations pooling information and making it available to each other.
- Several organisations pooling information and making it available to a third party or parties.
- Exceptional, one-off disclosures of data in unexpected or emergency situations.
- Different parts of the same organisation making data available to each other.

Some data sharing doesn't involve personal data, for example where only statistics that cannot identify anyone are being shared. The Data Protection Act (DPA) does not apply to that type of sharing.

The first data protection principle states that organisations have to satisfy one or more 'conditions' in order to legitimise their processing of personal data, unless an exemption applies. For instance:

a) **Consent** or explicit consent for data sharing is most likely to be needed where:

- Confidential or particularly sensitive information is going to be shared without a clear legal basis for doing so.
- The individual would be likely to object should the data be shared without his or her consent.
- Or the sharing is likely to have a significant impact on an individual or group of individuals.

b) The processing is **necessary**:

- In relation to a contract which the individual has entered into.
- Because the individual has asked for something to be done so they can enter into a contract.

c) The processing is necessary because of a **legal obligation**

d) The processing is necessary to protect the individual's **"vital interests"** (you can process personal data if it's necessary to protect someone's life. This could be the life of the data subject or someone else).

e) The processing is necessary for a "**public task**" such as administering justice, or for exercising statutory, governmental, or other public functions.

- if you are required by UK or EU law to process the data for a particular purpose

f) The processing is in accordance with the **"legitimate interests"** condition:

- The 'legitimate interests' condition provides grounds to process personal data in a situation where an organisation needs to do so for the purpose of its own legitimate interests or the legitimate interests of the third party that the information is disclosed to.
- This condition cannot be satisfied if the processing is unwarranted because it prejudices the rights and freedoms or legitimate interests of the individual whose data is being processed.
- This condition cannot legitimise the processing of sensitive personal data.

2.10 Guidance for Handling a Data Breach and Prevent Cyber Attacks

A data breach occurs when a breach of security has led to accidental or unlawful destruction, loss, alteration or unauthorized disclosure of personal data. It could include the following;

- The disclosure of confidential data to unauthorized individuals.
- The loss or theft of equipment containing personal information
- Leaving IT unattended
- Inappropriate access controls
- Misdirected emails
- The loss or theft of paper records
- Cyber-attacks such as phishing or malware that result in data access

Sufra NW London staff and volunteers should report a data breach to their line manager and complete a Data Protection Breach Form.

Take immediate steps to minimise further data exposure, such as:

- Resetting passwords
- Logging out of all active sessions or devices
- Keep devices and software up to date by installing updates and ding a scan for viruses
- Recalling or deleting a misdirected email (if possible)
- Restricting access to affected files or systems

If the breach is not reported it could have significant detrimental effects on individuals – for example, it can result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Sufra is required to report to the ICO (Information Commissioner's Office) within 72 hours, where the breach is likely to result in a risk to the rights and freedoms of individuals. It is therefore important that any personal data breach is reported to the Data Protection Team as soon as possible after they occur. A serious data breach may also be reported to the Charity Commission.

If Sufra fails to notify the ICO of such a breach can result in a significant fine.

If the data breach poses a high risk to the individuals affected, Sufra would also be required to report certain types of data breach to the individuals affected.

When you report the data breach to your Line Manager, an assessment of the data breach will be made to see if this would be required. All breaches—whether reported to the ICO or not—should be documented internally, as per Article 33(5) of the UK GDPR and response actions recorded in a log.

With an increased reliance on electronic devices now more than ever, we are committed to upholding strong cyber security to keep our data protected. We have numerous measures in place to protect against cyber attacks. Staff should ensure that they are;

- Keeping devices and software up to date;
- Using devices with appropriate antivirus and antimalware software;
- Only using secure internet connections
- Using strong passwords and multi-factor authentication
- Using devices that are securely configured and requiring login before use.
- Have restricted views and admin functions (where appropriate)

2.11 Guidance for collecting data via CCTV surveillance

In order to keep Sufra staff, guests and resources safe, Sufra captures CCTV footage of our main premises and garden premises.

The Facilities and Logistics Manager is responsible for CCTV operations and managing footage view requests. Access to footage is limited and is saved on a hard drive device and on cloud storage for 30 days.

Sufra NW informs staff, guests and visitors that CCTV is in operation by displaying notices on the premises.

3 Rights of Individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

3.1 Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

3.2 Right of access

- Enabling individuals to access their personal data and supplementary information.
- Allowing individuals to be aware of and verify the lawfulness of the processing activities.

3.3 Right to portability

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

3.4 Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

3.5 Right to erasure / to be forgotten

- When data is provided on the lawful basis of consent, we must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.
- If data is held on the lawful basis of legitimate interest, we will erase data if there is no overriding legitimate interest for us to continue with the processing.

3.6 Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.

3.7 Right to restrict processing

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, you are permitted to store the personal data but not use it.

4 Subject Access Requests

If an individual contacts the charity requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Charity at admin@sufra-nwlondon.org.uk. Staff should respond by sending a Subject Access Request form as soon as possible, located in OneDrive under: General > Forms & Templates.

The charity will aim to provide the relevant data within one calendar month.

Individuals may be charged a fee for subject access requests that are excessive or particularly complex.

Sufra can decide to refuse a subject access request where it is clearly or obviously unreasonable. Should Sufra NW London decide to refuse all or part of the request, staff should document our reasons for the refusal and share this decision with the individual requesting access.

The charity will always verify the identity of anyone making a subject access request before handing over any information. Where files also hold information about third

parties, Sufra will ensure that the identity of the third parties cannot be found through the information you share.

5 Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Sufra NW London will disclose requested data. However, the charity will ensure the request is legitimate, seeking assistance from the Board and from the external legal advisers where necessary.

To these ends, the charity has a detailed privacy statement, setting out what data we collect, how data relating to individuals is used by the charity and more.

[END]

BOARD APPROVED 04.06.2025

Reviewed May 2025

Reviewed: 26 May 2023

Revised 5 August 2020

APPENDIX A: Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is required before starting any project or activity that could pose a high risk to individuals' privacy or data rights. This includes using CCTV, processing sensitive data (like health or ethnicity information), working with vulnerable groups (e.g. children), or using new technologies such as profiling or automated decision-making.

DPIAs help us identify and reduce privacy risks, ensure we meet our legal obligations under the UK GDPR, and demonstrate accountability. Completing a DPIA is essential to protect both our service users and the organisation.

A Data Protection Impact Assessment (DPIA) isn't required when data processing is low risk—for example, if it doesn't involve sensitive data, vulnerable individuals, new or intrusive technology, or large-scale monitoring. You also don't need one if a similar activity has already been assessed. If you're unsure, always check with the Data Protection Officer (DPO).

Organisation: Sufra NW London
Date Completed: [Insert Date]
Completed by: [Insert Name and Role]
Reviewed by DPO: [Insert Name and Date]

◈ 1. Project Overview

Project title: [Name]

Description of the project or processing activity:

Briefly describe the nature, scope, context and purposes of the processing. Include the data flow (collection, use, storage, deletion).

◈ 2. Purpose and Legal Basis

What is the purpose of the data processing?

e.g. “To receive, process and monitor referrals electronically from partner agencies for more efficient service provision.”

What is the legal basis for processing under UK GDPR (please highlight):
Consent
Contract

Legal Obligation
Vital Interests
Public Task
Legitimate Interests

If Legitimate Interest then a Legitimate Interest Assessment is needed.

◈ 3. Categories of Personal Data

Types of data collected (please highlight):
Name
Contact details
Ethnicity
Health/disability information
Other: [specify]

Are any special category or criminal offence data processed (please highlight)?
Yes
No

If yes, explain necessity and safeguards in place.

◈ 4. Data Subjects

Who are the individuals affected?
Service users
Children/young people
Staff
Volunteers
Donors
Others: [specify]

◈ 5. Data Flow and Storage

How is the data collected?

e.g. “Via online referral forms completed by partners”

Where is the data stored?

e.g. “Secure Advice Pro database, UK-based cloud servers (Microsoft OneDrive)”

Who has access to the data?

e.g. “Caseworkers, referral coordinator, IT support (restricted access)”

How long is the data retained?

Cross-reference to your retention schedule.

◈ 6. Risks to Individuals

Potential risks to data subjects:

- Unauthorised access to sensitive data
- Accidental loss or deletion of case files
- Misuse of health or ethnicity data
- Re-identification from anonymised datasets

◈ 7. Measures to Minimise Risk

What safeguards are in place (please highlight)?

Secure access controls (passwords, role-based permissions)

Encryption of data in transit and at rest

Staff/volunteer training

Use of secure servers and devices

Data minimisation and pseudonymisation

Written data sharing agreements (where applicable)

◈ 8. Rights of Individuals

How will individuals be informed about their rights?

e.g. “Via a privacy notice issued at the point of referral and available on our website”

How will individuals exercise their rights (access, rectification, erasure, objection)?

“Through submission of a Subject Access Request (SAR) via our website or directly to admin@sufra-nwlondon.org.uk.”

◈ 9. Decision and Actions

Proceed with processing as planned
Proceed with changes (specify)
Do not proceed with processing

Actions required before implementation:

- Complete privacy notice
- Finalise data sharing agreement
- Conduct staff training
- Ensure encryption and back-up protocols are in place

Sign-off

Project Lead Name: _____
Signature: _____
Date: _____

Data Protection Officer Name: _____
Signature: _____
Date: _____

5.1.1 APPENDIX B: LEGITIMATE INTERESTS ASSESSMENT (LIA)

Organisation: Sufra NW London

Purpose of Processing:
To collect and analyse service user data (e.g. Food Bank visits) to improve service delivery, monitor demand, and report to funders.

1. Purpose Test – Is there a legitimate interest?
Yes. The processing supports Sufra's aim to deliver responsive and effective services and meet funder requirements.

2. Necessity Test – Is the processing necessary?
Yes. We need identifiable data to track usage patterns, avoid duplication, and ensure appropriate support. Anonymised data alone is insufficient.

3. Balancing Test – Is the impact on individuals minimal and justified?
Yes. The data collected is limited, stored securely, and only accessible to trained staff. Individuals are informed via our privacy notice and can request data to be anonymised for reporting.

Outcome (please highlight):
Legitimate interests apply.
Additional safeguards needed.
Do not proceed.

Approved by DPO:
Name: _____
Date: _____