GREATER**LONDON**AUTHORITY

[redacted]
(by email)

Our Ref: MGLA280120-1421

24 February 2020

Dear [redacted]

Thank you for your request for information which the Greater London Authority (GLA), received on 28 January 2020. Your request has been considered under the Freedom of Information Act (FOIA) 2000.

You requested:

> *1) copies of any current data protection/information sharing policies and protocols held by the GLA that relate to the commissioned No Second Night Out Service; and*
> *2) copies of any consent forms or privacy information notices relating to NSNO.*

Please find attached the information we hold within the scope of your request.

A small amount of information that relate to names of staff are exempt from disclosure under section 40 of the FOIA. This information could potentially identify specific employees and as such constitutes as personal data which is defined by Article 4(1) of the General Data Protection Regulation (GDPR) to mean any information relating to an identified or identifiable living individual.

If you have any further questions relating to this matter, please contact me, quoting the reference MGLA300120-1531.

Yours sincerely,

[redacted]
Senior Information Governance Officer

If you are unhappy with the way the GLA has handled your request, you may complain using the GLA's FOI complaints and internal review procedure, available at:
https://www.london.gov.uk/about-us/governance-and-spending/sharing-our-information/freedom-information

Explaining your information rights at No Second Night Out

Your rights

St Mungo's recognises your rights to data including the following:

- ***The Right of Access to personal data -*** You are able to request all information which St Mungo's holds on you. This will include what information we hold, why we hold it and if we are sharing it. You can do this by contacting your service manager, or contact our Information Security team directly using the details below.
- ***The Right to be Informed –*** St Mungo's will help you understand any complex terms or codes on your record by providing explanations where needed. We would encourage you to ask questions to help you understand your record including why we hold types of information and what we use it for. We will also let you know if we do not hold some information you have requested
- ***The Right to Accuracy*** – If you see something on your record you believe is inaccurate you can request we amend it. St Mungo's will need to demonstrate they have checked the information and ensure accuracy is maintained to the best of our knowledge.
- ***The Right to Erasure/Restriction*** – You can ask St Mungo's to remove information or to stop using some of your information. We will consider your request against the purpose and legal basis for holding your data. There may be some cases where we cannot remove data, or where erasing it would prevent us being able to continue working with you. In these cases we will explain the reasons clearly and advise you on the options available to you.

Being clear about you and your information at No Second Night Out

We collect personal and sensitive information from you to ensure we are able to provide you with the most appropriate and tailored support.

What is collected will vary between services and projects so you may have some information which is used for different reasons. This document will explain those reasons, and should answer any other questions.

If you have any questions about how your information is used you can ask your service manager, keyworker or contact Information Security at St Mungo's using the details below. We will be more than happy to help and answer any questions you may have.

Your Personal Information

We ask you for your Name, Date of Birth, immigration and economic status and Identification numbers (NI, passport, housing benefit reference, NHS number).

This information is collected to confirm your identity and better understand which services and benefits you are able to access. We also use this to ensure we are delivering a fair and inclusive service.

We also collect more general information about you to better understand the sort of support you might need. This could include whether you're a parent, your education history, and boroughs or cities you have a local connection with.

We use this extra information to help us provide targeted support to you around the areas which are most important to you in fulfilling your hopes and ambitions.

Your Sensitive Information

- **Racial or Ethnic origin and Religious or philosophical beliefs**
  Recorded to assess your entitlements and eligibility to specialised support services, benefits and public funds. This information will never be used to discriminate against you. It may also be used for reporting on our services, but this would be done anonymously.

- **Mental and physical health diagnoses and well-being**
  We initially receive this information in referrals. This is used to assess accommodation and plan appropriate support before your arrival. This could involve contacting and sharing information with relevant agencies already working with you. We will also do this if we believe there may be undiagnosed conditions.

- **Details of drug and alcohol use, support and any related incidents**
  This information is used to understand whether or not there are any support needs we should be aware of to provide the right support and to minimise risk or harm to yourself and others. It is also used to assess any patterns of behaviour to help provide better support.

- **If you are a victim or have support needs around domestic violence**
  We record this information to make sure we can support any needs you may have.

- **Sexual behaviour and orientation**
  This information is used particularly to provide harm minimisation and support.

- **Information about offending history and behaviour**
  We may receive information from the criminal justice system or from the police. Only the relevant risk information will be stored.
  These checks are done to keep every safe including yourself, other clients and staff. This information will not be used to discriminate against you, and we will never share these details externally without your clear and explicit consent.

We collect this information for five main reasons:

1) To identify any specific support or services you might be eligible for
2) To ensure we are providing you with a fair and inclusive service
3) To manage any risk to yourself, other clients, staff, the public and the environment appropriately
4) To evidence that we are delivering on our contracts with those who commission and fund our projects and services
5) To assess our own performance and provisions of services so that we can continuously improve

Where we are using the last two reasons, we will make sure to minimise your personal information so that the information cannot reasonably be linked back to you.

In exceptional circumstances, for example, if we have safeguarding concerns, we may also have to use your information to effectively manage any risks to vulnerable adults and/or children.

What are our legal reasons for processing your information?

No Second Night Out does not collect any of your information using consent. This is because there is some information we need to process so that you can stay at and engage with No Second Night Out

We process information under four legal bases:

1) We collect the majority of your personal and sensitive information under the legal basis of **(Substantial) Public Interest.** We will only use this information for the purposes as stated above. If you have concerns about your data, we promise to listen and support you around these.
2) **Legitimate Interest**. For example, this may include your parental or grandparental status, details about previous accommodation, and your phone number. If you are not happy for us to store this information, we are able to remove it at any time.
3) Sometimes we need to process information to protect **Vital Interests.** This means we may have to share, collect or otherwise use your information to protect the life of yourself or others.

Sharing your information

We have to share information between ourselves and other agencies to provide combined support. There are some agencies which we work more closely with, below is a list of these agencies, grouped according to why we would share your information.

- Housing authorities
- Previous and prospective housing providers
- Advice agencies for example housing and welfare advice providers; drug and alcohol support services
- Your social worker
- National Records Office or Embassy to obtain ID

- Your Community Mental Health Team and other mental health professionals
- Your current and/or past GPs / doctors
- Hospitals that have information relevant to your housing
- Your current and/or past probation or other criminal justice professionals

The names of any agencies falling under the last four points in this list will be clearly documented and available on request.

How long will we keep your data?

We will keep your data for a period of **three years**, after you have left the service. Your data will then be minimised and only the following information will be kept:

- Your name and date of birth to identify you should you re-engage with a St Mungo's service in the future.
- A list of the services you engaged with including dates of entry and exit, again this would be able to help us better support you should you re-engage.

In some exceptional cases we may have to keep additional information. This will only be done if there were any significant risks to yourself, other clients, staff, the public and the environment which we'd need a record of, should you re-engage.

This information will only be kept for a maximum of **seven years** after you have left the service.

Queries and complaints

For any queries or complaints regarding the use of your data please contact any of the below who will be able to assist you.

St Mungo's

Service manager
Name
Role, Service
Email
Number

Information Security Team
Data Protection Officer
InfoSec@mungos.org
Tel: 020 3856 6121
Write: Information Security, St Mungo's, 3 Thomas More Square, Tower Hill, London, E1W 1YW

Complaints
complaints@mungos.org
Tel: 020 3856 6068
Write: Quality team, St Mungo's, 3 Thomas More Square, Tower Hill, London E1W 1YW.
Please note - we are unable to see personal callers at this address

If you are not happy with the response you receive from St Mungo's, you can contact the UK representative for data protection.
The Information Commissioner's Office
www.ico.org.uk
0303 123 1113

Data Protection Policy

Policy statement

Thames Reach collects and uses personal data in order to carry out its legitimate business practices. We are committed to protecting the rights and freedoms of people whose data we process and safely and securely processing their data in accordance with all current legal obligations.

Personal data is any information that relates to an identified or 'identifiable natural person'. Thames Reach holds personal data about its employees, service users, supporters and donors for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of personal information in the course of their work.

This policy is in line with the General Data Protection Regulations (GDPR), which came into force on 25th May 2018 and subsequent Data Protection Act 2018.

Scope

The Thames Reach senior manager responsible for data protection is the Director of Finance and Central Services. Day-to-day implementation of this policy is the responsibility of the Leadership Team.

Thames Reach has compiled a list of its data processes covering areas such as processing purposes, data sharing, retention periods, security and the legal bases that best apply to each processing purpose. See the 'Data Register' (Schedule 1) and associated Data Security policy.

This policy applies to all board members, staff and volunteers, who are required to read, understand and accept all policies and associated procedures that relate to the personal information they may handle in the course of their work.

The principles

Thames Reach shall comply with the principles of data protection detailed in the EU General Data Protection Regulations. We will make sure that personal data is:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Kept for no longer than is necessary
- Processed in a manner that ensures appropriate security of the personal data

All Thames Reach staff must understand the importance of these principles and always ensure that their processing of personal data is in-line with them.

Data Controlling and Data Processing

As an employer, and in our fundraising and business development work, Thames Reach considers itself primarily a Data Controller, in that it determines the purpose and means of processing personal data. However, we also recognises that there will be occasions where we act as a Data Processor on behalf of a Data Controller, for example, when delivering a commissioned service on behalf of a local authority and when acting as a managing agent for a Registered Landlord.

As a Data Processor, Thames Reach will comply with all contractual obligations and act only on the documented instructions contained in the management contract. We will also ensure that all sub-processors operate with the terms of the contract.

Lawful basis for processing data

The GDPR requires that Data Controllers establish a lawful basis for processing data. At least one of the following conditions must apply whenever personal data is processed:

Consent: the individual has given clear consent for us to process their personal data for a specific purpose

Contract: the processing is necessary for a contract that we have with the individual, or because they have asked us to take specific steps before entering into a contract

Legal obligation: the processing is necessary for us to comply with the law

Vital interests: the processing is necessary to protect someone's life

Public task: the processing is necessary for us to perform a task in the public interest or for our official function, and the task or function has a clear basis in law

Legitimate interests: the processing is necessary for our 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

Thames Reach will publish the legal bases used for processing personal data via a privacy notice to ensure that individuals whose data is being processed by us are informed about the way in which we use, share and store personal information. The privacy notice will ensure that where necessary individuals can give informed consent for our use of their data.

Special categories of personal data

Thames Reach recognises that the processing of particular information is more sensitive and so requires more protection. This type of 'special category' data could create more significant risks to a person's fundamental rights and freedoms. The special category data includes information about an individual's: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health and sexual orientation.

Thames Reach will only process special categories of data where the individual expressly consents to such processing, or where it is based on its legitimate business activity, i.e. where demographic monitoring is a condition of funding.

The condition for processing special categories of personal data must always comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity will cease.

Criminal offence data

All data relating to criminal convictions and offences, including data about allegations and criminal proceedings, is considered to be a special category data and must be treated as such.

Processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by UK law. Criminal record checks cannot be undertaken based solely on the consent of the individual. We will not keep a comprehensive register of criminal offence data.

Children's data

There are occasions where Thames Reach will process the data of individuals under the age of 18, for example a 16/17 year old service user living as an adult, the children of current service users and young donors to the charity. Children need particular protection when collecting and processing their personal data because they may be less aware of the risks involved.

For 16/17 year olds living as adults we will assess the risks of processing their data and will only process on the basis of consent or delivery of a contract if we can be certain that they fully understand the nature of the arrangement. Processing of data for anyone under 16 will only be done with the consent of a parent or guardian.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them.

Consent

Where Thames Reach uses consent as its legal basis, we will ensure that it is unambiguous and involves a clear affirmative action (an opt-in). Consent forms will state clearly what the data will be used for and how long the consent is valid. We will build regular consent reviews into our practice and ensure that consents are refreshed periodically. Thames Reach will keep clear records to demonstrate that consent has been given.

Direct marketing

Thames Reach believes that it is a legitimate business practice for it to market itself to potential funders and supporters. Thames Reach will, in some circumstances, send marketing information by post to potential new supporters under the legal basis of legitimate interest but will always be sensitive to the nature and frequency of that communication and will ensure that the individual knows how they can object to their data being used in this way.

Where staff or service user data is used in marketing materials it will only be done under the legal basis of consent.

Data security

We will keep personal data secure against loss or misuse. In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it. Printed data will be shredded when it is no longer needed.

Data stored on a computer will be protected by strong passwords that are changed regularly. The Thames Reach Information Sharing and Security policy covers password use, procedures for securing unattended computers, accessing information off-site and the use of personal devices for work activity. Data stored on CDs or memory sticks will be encrypted or password protected and locked away securely when they are not being used.

Data that is no longer required will be deleted from all filing and storage systems

Rights of individuals

This policy provides the following rights for individuals:

Right to be informed - We will provide individuals with information including: the purposes for processing their personal data, retention periods for that personal data, and who it will be shared with.

Right of access - We will provide individuals with access to our records to allow them to see and verify the lawfulness of our processing.

Right to rectification - Individuals have the right to have inaccurate personal data rectified. An individual may also request that incomplete personal data be completed.

Right to erasure (also known as the right to be forgotten) - Individuals have the right to have personal data erased in certain circumstances.

Right to restrict processing - Individuals have the right to restrict the processing of their personal data in certain circumstances.

Right to data portability - We will provide, on request, copies of personal data held by Thames Reach in a structured, commonly used and machine readable format allowing them to reuse their personal data for their own purposes across different services.

Right to object - Individuals have the right to object to processes based on legitimate interests or the performance of a task in the 'public interest', direct marketing (including profiling) and processing for purposes of scientific/historical research and statistics.

Fees and timescales - In normal circumstances the above rights will be provided free of charge. Where requests are considered manifestly unfounded or excessive, Thames Reach will consider whether a reasonable fee should be charged taking into account the administrative costs of undertaking the task.

Information must be provided without delay and at the latest within one month of receipt of the request.

Reporting breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioner's Office (ICO). This must be done within 72 hours of becoming aware of the breach, where feasible.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Breaches within Thames Reach should be reported internally using the Serious Incident Reporting procedure.

Serious breaches should be reported to the ICO via this link:

https://ico.org.uk/for-organisations/report-a-breach/

Training

All Thames Reach employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, Thames Reach will provide additional training for particular categories of staff, i.e. managers, support staff, database administrators etc. as required.

Failure to comply

Thames Reach takes compliance with this policy very seriously. Failure to comply puts both the individual member of staff and the organisation at risk. Failure to comply with any part of this policy may lead to disciplinary action being considered.

GREATER LONDON AUTHORITY

Contract Reference Number: GLA 80838

Contract for Services

between

The Greater London Authority (GLA)

and

For the Provision of No Second Night Out (NSNO)

Version: Generic 24 July 2015

SCHEDULE 2 - SPECIAL CONDITIONS OF CONTRACT

A1 Privacy and Data Protection

For the purposes of this Clause A1, unless the context indicates otherwise, the following expressions shall have the following meanings:

"Authority Personal Data"	Personal Data and/or Sensitive Personal Data Processed by the Service Provider on behalf of the Authority;
"Data Controller"	has the meaning given to it by section 1(1) of the Data Protection Act 1998;
"Data Processor"	has the meaning given to it by section 1(1) of the Data Protection Act 1998;
"Data Subject"	has the meaning given to it by section 1(1) of the Data Protection Act 1998;
"Data Protection Legislation"	the Data Protection Act 1998 (as interpreted in accordance with Directive 95/46/EC) including all regulations made under it and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any amendment or re-enactment of any of them; any other legislation relating to privacy and/or the processing of Personal Data (as amended from time to time); and any guidance or statutory codes of practice issued by the Information Commissioner in relation to such legislation;
"Personal Data"	has the meaning given to it by section 1(1) of the Data Protection Act 1998;
"Privacy Impact Assessment"	a process used to identify and mitigate the privacy and data protection risks associated with an activity involving the Processing of Authority Personal Data.
"Processing"	has the meaning given to it by section 1(1) of the Data Protection Act 1998 and **"Process"** and **"Processed"** will be construed accordingly;
"Restricted Countries"	any country outside the European Economic Area; and
"Sensitive Personal Data"	has the meaning given to it by section 2 of

	the Data Protection Act 1998; and
"Subject Access Request"	a request made by a Data Subject to access his or her own Personal Data in accordance with rights granted pursuant to Data Protection Legislation.

A1.1 With respect to the Parties' rights and obligations under the Contract, the Parties acknowledge that the Authority is a Data Controller and that the Service Provider is a Data Processor.

A1.2 Details of the Authority Personal Data to be Processed by the Service Provider and the purposes of such Processing are as follows:

A1.2.1 Categories of Data Subject

The Authority Personal Data to be processed by the Service Provider (if any) concerns the following categories of Data Subjects:

- *staff;*
- *service users;*
- *volunteers; and*
- *other rough sleepers.*

A1.2.2 Categories of Authority Personal Data

The Authority Personal Data to be processed concerns the following categories of Personal Data and/or Sensitive Personal Data:

- *name;*
- *address;*
- *telephone number;*
- *photograph;*
- *age;*
- *gender;*
- *physical description;*
- *national insurance number;*
- *identity card number; and*

- *passport number.*

A1.2.3 Purpose(s) of the Processing

The Authority Personal Data is to be processed for the following purpose(s):

*The delivery of the Services; research, service development and planning.*A1.2.4 Permitted offshore processing

The Authority Personal Data is to be processed in the following Restricted Countries:

No request was made by the Service Provider to process Authority Personal Data in any non EEA Country.

A1.3 Without prejudice to the generality of Clause 22, the Service Provider shall:

A1.3.1 process the Authority Personal Data only in accordance with instructions from the Authority to perform its obligations under the Contract;

A1.3.2 use its reasonable endeavours to assist the Authority in complying with any obligations under Data Protection Legislation and shall not perform its obligations under this Contract in such a way as to cause the Authority to breach any of its obligations under Data Protection Legislation to the extent the Service Provider is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations;

A1.3.3 maintain, and make available to the Authority on its request, documentation, a central register or an inventory which describes the Processing operations for which it is responsible and specifies: the purposes for which Authority Personal Data are processed including the legitimate interests pursued by TfL where processing is based on this lawful basis; the categories of Personal Data and Data Subjects involved; the source of the Personal Data; the recipients of the Personal Data; and the location(s) of any overseas processing of those Personal Data;

A1.3.4 take appropriate technical and organisational security measures, that are satisfactory to the Authority from time to time, against unauthorised or unlawful Processing of Authority Personal Data and against accidental loss, destruction of, or damage to such Authority Personal Data;

A1.3.5 without prejudice to Clause A1.3.4, wherever the Service Provider uses any mobile or portable device for the transmission or storage of Authority Personal Data, ensure that each such device encrypts Authority Personal Data;

A1.3.6 provide the Authority with such information as the Authority may from time to time require to satisfy itself of compliance by the Service Provider (and/or any authorised sub-contractor) with Clauses A1.3.4 and A1.3.5, including, protocols, procedures, guidance, training and manuals. For the avoidance of doubt, this shall include a full report recording the results of any privacy or security audit carried out at the request of the Service Provider itself or the Authority;

A1.3.7 where requested to do so by the Authority, or where Processing Authority Personal Data presents a specific risk to privacy, carry out a Privacy Impact Assessment in accordance with guidance issued from time to time by the Information Commissioner (and any relevant statutory requirements) and make the results of such an assessment available to the Authority;

A1.3.8 notify the Authority within two (2) Business Days if it, or any Sub-contractor, receives:

A1.3.8.1 from a Data Subject (or third party on their behalf):

A1.3.8.1.1 a Subject Access Request (or purported Subject Access Request);

A1.3.8.1.2 a request to rectify, block or erase any Authority Personal Data; or

A1.3.8.1.3 any other request, complaint or communication relating to the Authority's obligations under Data Protection Legislation;

A1.3.8.2 any communication from the Information Commissioner or any other regulatory authority in connection with Authority Personal Data; or

A1.3.8.3 a request from any third party for disclosure of Authority Personal Data where compliance

with such request is required or purported to be required by law;

A1.3.9 provide the Authority with full cooperation and assistance (within the timescales reasonably required by the Authority) in relation to any complaint, communication or request made as referred to in Clause A1.3.8, including by promptly providing:

A1.3.9.1 the Authority with full details and copies of the complaint, communication or request; and

A1.3.9.2 where applicable, such assistance as is reasonably requested by the Authority to enable it to comply with the Subject Access Request within the relevant timescales set out in Data Protection Legislation.

A1.3.10 when notified in writing by the Service Provider, supply a copy of, or information about, any Authority Personal Data. The Service Provider shall supply such information or data to the Authority within such time and in such form as specified in the request (such time to be reasonable) or if no period of time is specified in the request, then within five (5) Business Days from the date of the request.

A1.3.11 when notified in writing by the Authority, comply with any agreement between the Authority and any Data Subject in relation to any Processing which causes or is likely to cause substantial and unwarranted damage or distress to such Data Subject, or any court order requiring the rectification, blocking, erasure or destruction of any Authority Personal Data;

A1.4 The Authority remains solely responsible for determining the purposes and manner in which Authority Personal Data is to be Processed. The Service Provider shall not share any Authority Personal Data with any sub-contractor or third party without prior written consent from the Authority (in the Contract or otherwise) and unless there is a written contract in place with the sub-contractor which requires the sub-contractor or third party to:

A1.4.1 only Process Authority Personal Data in accordance with the Authority's instructions to the Service Provider; and

A1.4.2 comply with the same obligations with which the Service Provider is required to comply with under this Clause A1 (and in particular Clauses 12.1, 16.1, 16.2, 18.1, 20.2, 22 and 23).

A1.5 The Service Provider agrees that, and shall procure that any sub-contractor shall agree that, Authority Personal Data:

A1.5.1 must only be Processed in accordance with the Authority's obligations to comply with Data Protection Legislation and by such their personnel as need to view or otherwise access Authority Personal Data;

A1.5.2 must only be used as instructed by the Authority and as reasonably necessary to perform the Contract in accordance with its terms;

A1.5.3 must not be used for any other purposes (in whole or part) by any of them (and specifically but without limitation must not be copied or referred to in whole or part through training materials, training courses, discussions or negotiations or contractual arrangements with third parties or in relation to proposals or tenders with the Authority (or otherwise), whether on renewal of this Contract or otherwise, without the prior written consent of the Authority); and

A1.5.4 must not be used so as to place the Authority in breach of Data Protection Legislation and/or to expose it to risk of actual or potential liability to the Information Commissioner, Data Subjects and/or reputational damage and/or to any order being made against the Authority preventing, suspending or limiting the Processing of Authority Personal Data.

A1.6 The Service Provider shall, and shall procure that any sub-contractor shall:

A1.6.1 not disclose or transfer Authority Personal Data to any third party or their own personnel unless necessary for the provision of the Services and, for any disclosure or transfer of Authority Personal Data to any third party, obtain the prior written consent of the Authority (save where such disclosure or transfer is specifically authorised under this Contract);

A1.6.2 notify the Authority within 24 hours by written notice with all relevant details reasonably available of any actual or suspected breach of security and/or of the Contract and/or Clause A1 in relation to Authority Personal Data including unauthorised or unlawful access or Processing of, or accidental loss, destruction or damage of any Authority Personal Data;

A1.6.3 keep the Authority properly and regularly informed consequently;

A1.6.4 fully cooperate with the reasonable instructions of the Authority in relation to the Processing and security of Authority Personal Data in accordance with the Contract and in compliance with Data Protection Legislation (including procuring access to sub-contractor premises);

A1.6.5 cooperate as the Authority requires with any investigation or audit in relation to Authority Personal Data and/or its Processing including allowing access to premises, computers and other information systems, records, documents and agreements as may be reasonably necessary (whether in relation to Processing pursuant to the Contract, in relation to Data Protection Legislation or in relation to any actual or suspected breach), whether by the Authority (or on its behalf) any relevant regulatory body, including the Information Commissioner, the police, any other statutory law enforcement agency or otherwise and shall do so both during the Contract and after its termination or expiry (for so long as the Party concerned retains and/or Processes Authority Personal Data);

A1.6.6 take all reasonable steps to ensure the reliability and integrity of all Service Provider's Personnel who can/or do access Authority Personal Data;

A1.6.7 ensure all Service Provider's Personnel who can/or do access Authority Personal Data are informed of its confidential nature and do not publish, disclose or divulge any of the Personal Data to any third party without the prior written consent of the Authority;

A1.6.8 ensure all Service Provider's Personnel who can and/or do access Authority Personal Data have undergone adequate training in relation to the use, care, protection and handling of Personal Data in accordance with Data Protection Legislation and this Contract, understand such obligations and comply with them and ensure that such training is updated at reasonable intervals; and

A1.6.9 comply during the course of the Contract with any written retention and/or deletion policy or schedule provided to it by the Authority from time to time.

A1.7 The Service Provider shall not, and shall procure that any sub-contractor shall not, Process or otherwise transfer any Authority Personal Data in or to any Restricted Countries without prior written consent from the Authority (which consent may be subject to additional conditions imposed by the Authority).

A1.8 If, after the Service Commencement Date, the Service Provider or any sub-contractor wishes to Process and/or transfer any Authority

Personal Data in or to any Restricted Countries, the following provisions shall apply:

A1.8.1 the Service Provider shall submit a written request to the Authority setting out details of the following:

A1.8.1.1 the Authority Personal Data which will be transferred to and/or Processed in any Restricted Countries;

A1.8.1.2 the Restricted Countries which the Authority Personal Data will be transferred to and/or Processed in;

A1.8.1.3 any sub-contractors or other third parties who will be processing and/or receiving Authority Personal Data in Restricted Countries;

A1.8.1.4 how the Service Provider shall ensure an adequate level of protection and adequate safeguards in respect of the Authority Personal Data that will be Processed in and/or transferred to Restricted Countries so as to ensure the Authority's compliance with Data Protection Legislation;

A1.8.2 in preparing and evaluating such a request, the Parties shall refer to and comply with applicable policies, procedures, guidance and codes of practice produced by the Parties and/or the Information Commissioner, in connection with, the Processing of Personal Data in (and/or transfer of Personal Data to) any Restricted Countries;

A1.8.3 the Service Provider shall comply with any instructions and shall carry out such actions as the Authority may notify in writing when providing its consent to such Processing or transfers, including:

A1.8.3.1 incorporating standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation) into this Contract or a separate data processing agreement between the Parties; and

A1.8.3.2 procuring that any sub-contractor or other third party who will be Processing and/or

receiving or accessing the Authority Personal Data in any Restricted Countries enters into a data processing agreement with the Supplier on terms which are equivalent to those agreed between the Authority and the Service Provider in connection with, the Processing of Authority Personal Data in (and/or transfer of Authority Personal Data to) any Restricted Countries, and which may include the incorporation of the clauses referred to in A1.8.3.1.

A1.9 The Service Provider and any sub-contractor (if any), acknowledge:

A1.9.1 the importance to Data Subjects and the Authority of safeguarding Authority Personal Data and Processing it only in accordance with the Contract;

A1.9.2 the loss and damage the Authority is likely to suffer in the event of a breach of the Contract or negligence in relation to Authority Personal Data;

A1.9.3 any breach of any obligation in relation to Authority Personal Data and/or negligence in relation to performance or non performance of such obligation shall be deemed a material breach of Contract;

A1.9.4 notwithstanding Clause 26.1.1, if the Service Provider has committed a material breach under Clause A1.9.3 on two or more separate occasions, the Authority may at its option:

A1.9.4.1 exercise its step in rights pursuant to Clause A16;

A1.9.4.2 withdraw authorisation for Processing by a specific sub-contractor by immediate written notice; or

A1.9.4.3 terminate the Contract in whole or part with immediate written notice to the Service Provider.

A1.10 If the Service Provider Processes payment card data under the Contract, it shall ensure that it is and that its internal processes and procedures, information technology systems and any equipment that it provides or is provided on its behalf pursuant to this Contract are compliant with the Payment Card Industry Data Security Standard as updated from time to time ("PCI DSS"). In addition the Service Provider shall:

A1.10.1 at least once every 12 months appoint a PCI DSS Qualified Security Assessor ("QSA") to validate that the Service Provider is compliant with (including as set out above) PCI DSS when providing the Services;

A1.10.2 without prejudice to any other audit and inspection rights that the Authority has under this Contract, provide the Authority with copies of any reports and other documents provided by or to the QSA in respect of each such validation; and

A1.10.3 where the QSA recommends that certain steps should be taken by the Service Provider, promptly take those steps and demonstrate to the Authority that those steps have been taken without charge to the Authority.

A1.11 Compliance by the Service Provider with this Clause A1 shall be without additional charge to the Authority.

A1.12 Following termination or expiry of this Contract, howsoever arising, the Service Provider:

A1.12.1 may Process the Personal Data only for so long and to the extent as is necessary to properly comply with its non contractual obligations arising under law (and will then comply with Clause A1.12.2);

A1.12.2 subject to Clause A1.12.1, shall;

(a) on written instructions from the Authority either securely destroy or securely and promptly return to the Authority or a recipient nominated by the Authority (in such usable format as and to the extent the Authority may reasonably require) the Authority Personal Data and relevant records and documentation accordingly; or

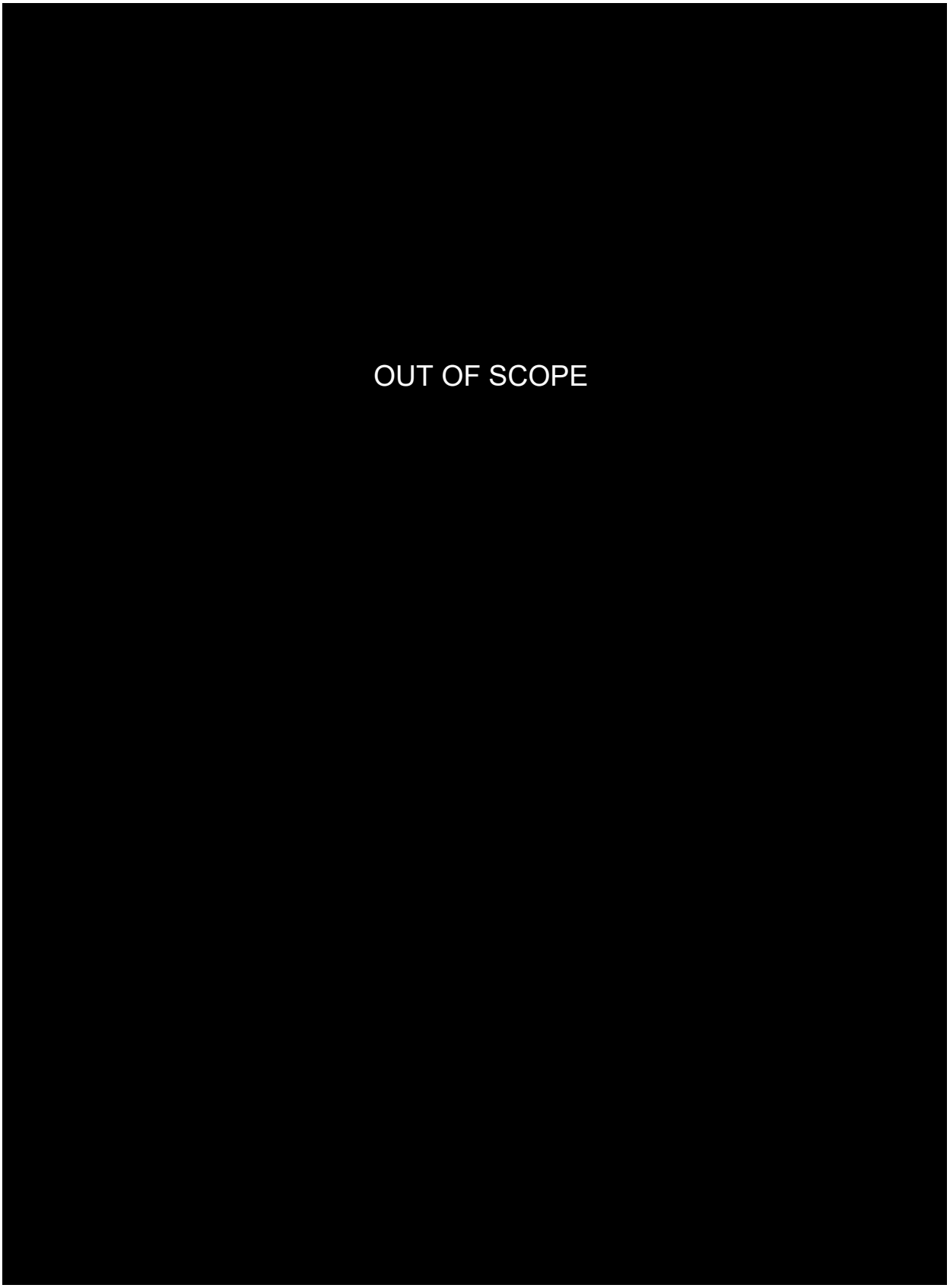
(b) in the absence of instructions from the Authority after 12 months from the expiry or termination of the Contract securely destroy the Authority Personal Data and relevant records and documentation accordingly.

Authority Personal Data may not be processed following termination or expiry of the Contract save as permitted by this Clause A1.12.

A1.13 For the avoidance of doubt, and without prejudice to Clause A1.12, the obligations in this Clause A1 shall apply following termination or expiry

of the Contract to the extent the Party concerned retains or Processes Authority Personal Data.

A1.14 The indemnity in Clause 18 shall apply to any breach of Clause A1 and shall survive termination or expiry of the Contract.



Information Sharing

Document reference: **J06**
Issue: **1**

Approved by: **Executive Director of Strategy & Policy**

[redacted]

Contents

Document Version Tracking

Version	Date	Revision Description	Editor	Status
1	22/02/2018	Initial version published	[redacted]	Published
2	28/06/2018	Minor Updates	[redacted]	Updated

Note: This document is electronically controlled. The master copy is maintained by InfoSec within MungosNet – always refer there for the latest version. Once printed, this document may fall out of date.

1. Policy

1.1. St Mungo's only ever processes identifying data for an expressed purpose and with a clear legal basis. This policy ensures that any data shared internally or externally is consistent with these purposes and at all times remains fair and legal.

1.2. Data sharing of all types is often an essential part of St Mungo's work. This policy is not intended to be a barrier to legitimate exchange, but instead is guidance to ensure St Mungo's properly safeguards and steward's data. St Mungo's recognises that excessive caution when sharing may cause as much disadvantage to data subject as carelessness. However serious harms and regulatory risk can occur from inappropriate disclosures. Instead, this policy contributes towards St Mungo's goals and Privacy by Design by:

(a) Providing procedures and guidance on how to recognise appropriate scenarios to share data, minimising the risk of breaking laws and receiving enforcement actions from the ICO or other regulators.

(b) Providing procedures on how relationships and sharing must be structured and documented, to ensure understanding from all parties on appropriate sharing, embed accountability procedures and ensure responsibilities are clearly defined.

(c) Providing procedures on how to share transparently, consistently and legally to increase the trust of client's, donors, staff and other data subjects. Through this we ensure appropriate safeguards and reduce the risk of unexpected questions, complaints or disputes about how personal data has been shared.

(d) Clarifying requirements on security and protection when sharing data. Reducing the risks of damage to data subject's as well as legal and reputational risks to St Mungo's.

(e) Reassuring staff when information sharing is necessary and beneficial, to ensure St Mungo's can effectively collaborate, contribute and safeguard those we work with.

1.3. St Mungo's has clear standards for information sharing, based on four core principles:

(a) **Fair and Legal** – All data must be collected and used with a clear legal basis (see *J04 – Legal Basis & Informed Consent*). Information we share must always be consistent with the legal basis and information on our purposes in privacy notices to the data subject. Information must never be shared (internally or externally) without a clear understanding of how the recipients intend to use it and if that usage is consistent.

(b) **Need to know basis** – With consideration to the purposes for which data was gathered, St Mungo's must ensure anything shared is strictly relevant to those purposes, proportionate to the task, adequate enough to allow a legitimate task to be accomplished and otherwise limited to what is necessary in relation to the processing. This is also known as data minimisation.

(c) **Secure** – That St Mungo's does not risk the security of data we steward by ensuring data transferred is appropriately secured/encrypted and by requesting assurances that other organisations and internal teams do not expose the data to unnecessary risk.

(d) **Documented & Auditable** – For any personal data St Mungo's uses, it must always be easy to establish and document whom the data has been shared with. St Mungo's must be prepared to respond to data subject requests detailing who has received their information, when it was shared, for what purpose and with what

justifications. This is a requirement arises in the right to be informed and must be auditable to the data subject through the right of access. St Mungo's must keep records of who made such decisions to ensure auditable trails in the case of disputes.

1.4. *J04 – Fair and Legal processing* and *J05 – Valid Consent* set standards that all staff must understand the legal basis for data they process. In addition this policy establishes the need for staff to be aware of who can establish this legal basis and set the purpose for use of data. This is established through assigning who is a Data Controller and a Data Processor in any relationship.

2. Key Terms and Definitions

2.1. **Data Sharing** – The act of disclosing data from one or more organisations (i.e. either St Mungo's alone or in partnership with others), to any third party organisation outside St Mungo's or other departments, teams, projects or services within St Mungo's.

2.2. **ICO** – The Information Commissioner's Office, the UK regulator on matters of data and privacy.

2.3. **Data minimisation** – The act of reducing the amount of information shared and used to the minimum possible to achieve your task. By doing so and keeping information on a 'need-to-know' basis, data minimisation reduces risks.

2.4. **Anonymisation** – The act of taking data that was once identifying and changing it so that it is impossible to recognise or pick out an individual, even by comparing the data any other potential sources.

2.5. **Pseudonymisation** – The act of taking data that was once identifying and changing it so that the identities of individuals are obscured, either by codes or by reducing the amount of identifying information. It is possible to re-identify this data, especially with reference to information from other sources, the level to which it is obscured should depend on the risk.

2.6. **Aggregate** – A calculated total created from data, for example added totals for a set of individuals. When aggregates are impossible to turn back into identifying data, it is also anonymised.

2.7. **DPA** – The Data Protection Act 2018. The legislation which determines much of our approach to the subject. See section 5.1 for further information.

2.8. **GDPR** – The General Data Protection Regulation. The new legislation which came into force in May 2018, which formalises many existing GDPR standards.

2.9. **Data Subject** - The Individual who is the subject of, or about who, St Mungo's processes data.

2.10. **Relevant Filing System** – Any repository of records that are held in a sufficiently systematic or structured way as to allow ready access to specific information about individuals,

2.11. **Processing** – means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

2.12. **Personally Identifying Data** – Data relating to a living individual who can be identified either from the data or from the data when combined with other information – be that from public sources or sources likely to come into the possession of the data controller.

2.13. **Sensitive Personal Data** – Categories granted enhanced protections given the content "could be used in a discriminatory way, and is likely to be of a private nature". Areas categorised as sensitive in the DPA can be found in Appendix 4 of P&P J02.

2.14. **Legal Basis** – The legal reason chosen from the lists within DPA or GDPR that is the legal justification for St Mungo's use of the data and that sets the limitations and what is allowed in the use of information.

2.15. **Data Subject** – the individual who is the subject of personal data and protections granted by the DPA. Valid data subjects must be, living and identifiable / distinguishable from other individuals to receive the protections of the DPA.

2.16. **Data Controller** – a person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

2.17. **Data Processor** – any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

2.18. **IAO** – Information Asset Owner is the senior member of staff or manager with responsibility for one or more repositories of personal identifying information. Asset Owners must be senior enough to implement changes in how the asset is handled, but sufficiently close that they understand it in detail.

2.19. **SAR** – Subject Access Request. A formal request from a data subject to view personal information held about them.

2.20. **Privacy Notice** – The combined set of materials that St Mungo's uses to inform individuals about how we use their information, their rights and our responsibilities. E.g. Posters, Organisational privacy policy and Information to Client forms. See *J08 – Privacy Notices*.

2.21. **Fair Processing Information** – Any individual piece of information that describes how St Mungo's use of data is fair and legal in line with data protection legislation.

3. Diversity Implications

3.1. This policy strengthens St Mungo's understanding of data subject rights and protects sensitive data by ensuring the respectful handling and sharing of information.

3.2. St Mungo's recognises the need for stewardship of data, especially where it stores sensitive personal data, noting the overlap with protected categories under the Equalities Act 2010. This policy helps mitigate the serious harms or discriminations that might be caused by inappropriate sharing or disclosure of sensitive information.

4. Scope

4.1. Data sharing concerns information shared externally, information shared within St Mungo's and information we receive as shared by a third party organisation. Data sharing can take the form of:

(a) A simple exchange of data. (E.g. an exchange of relevant support information between managers).

(b) St Mungo's providing data to a third party (e.g. providing data to a commissioner, reporting a safeguarding concern to a local authority, reporting a crime to the police).

(c) St Mungo's pooling data with other organisations and making it available to each other (e.g. shared databases between St Mungo's and other sector organisations).

(d) St Mungo's pooling data with other organisations and making it available to third parties (e.g. shared databases which are also accessible to commissioners or those who do not contribute data themselves).

(e) Exceptional one-off sharing in unexpected or emergency situations (e.g. providing details on a client or staff members health conditions to paramedics).

(f) Sharing of data within St Mungo's to different parts of the organisation, be that between team members, services or projects or across directorates.

(g) St Mungo's sending or receiving information at the beginning or end of a contract. Including TUPE scenarios.

4.2. These requirements only apply to personally identifying (see definition 2.12) and sensitive personally identifying (see 2.13) information. Other St Mungo's information such as business sensitive information, organisational financial information falls outside of the scope of this guidance. Sharing of this information should always consider the interests of St Mungo's and potential for reputational, commercial or financial damage with reference to the Code of Conduct and IT acceptable use standards.

4.3. Information that has been anonymised to the extent that it is impossible to transform back into personally identifying data can also be considered in line as non-identifying (in line with 4.2). However extreme care must be taken to ensure data has truly been anonymised and distinguish data that is pseudonymised. Section 7 provides further guidance in these areas.

4.4. Information sharing can fall into one of two broad categories:

(a) **Systematic sharing** – any routine, organised or foreseeable data sharing for an established purpose either internal to St Mungo's or with external organisations.

(b) **Exceptional sharing** – any one-off, ad-hoc or otherwise unforeseeable sharing that might be for a range of purposes, often as a response to an emergency or urgent consideration.

4.5. Any sharing, internally/externally, systematic/exceptional, at our request or at the request of another (e.g. a commissioner) must always remain consistent with the legal basis and purpose for which it was collected, or clearly connected to an exemption for an emergency purpose. Where this is not possible, a new legal basis must be established before sharing and the data subject informed. If the legal basis is consent they must also re-consent to the sharing. If these criteria cannot be fulfilled St Mungo's must not share the data.

4.6. When sharing data, all parties must be clear on who holds responsibilities around data protection and who is in control of the data, and how any new control or responsibilities organisations might gain through the sharing. Under data protection law there are two key concepts:

(a) **Data Controllers** – This person or organisation sets the clear purposes and holds responsibility for ensuring that the rights of data subjects are met and appropriate technical and organisational safeguards are in place to secure it.

Anywhere that St Mungo's collects data or receives data from another organisation (including commissioners), and is allowed professional discretion over how data is used. St Mungo's will be a data controller. St Mungo's must have similar expectations of organisations who receive our information for legitimate reasons.

(b) **Data Processors** – This is an organisation who receives data from a controller for a clear task and with express instructions on how to perform it. Data Processors have little professional discretion and must precisely follow the orders of the controller. These details must always be established in a clear contract that follows the guidance of *J08 – Data Sharing Agreements Section 5* and *Section 6*.

St Mungo's may often subcontract other organisations or even individuals who are not staff of St Mungo's to process data (e.g. mailing campaigns for donors, hosting or platforms for online systems, IT infrastructure). St Mungo's may also occasionally be contracted by another organisation or individual to perform a specific activity with access to their data. In either case the relationship and appropriate guarantees must always be clearly documented in a legally binding contract.

4.7. Responsibilities for data protection must be clearly established in contracts where relationships with external organisations exist and sharing is on a systematic basis. *J08 – Data Sharing Agreements*, provides further guidance on these documents.

4.8. The territorial scope of the General Data Protection Regulation extends to any non-EU organisation who is processing data about an EU citizen, especially where:

(a) The organisation is *"offering goods or services"* (payment is not required.

(b) EU citizens have their behaviour within the EU "*monitored*"

Any organisation that St Mungo's works with - or is commissioned to provide a service - outside of the EU, must therefore be able to meet all GDPR requirements, including those relating to data sharing. Otherwise St Mungo's must not provide them with personal data.

5. Deciding to share personal data

5.1. Any request to share information with anyone who is not verifiably the data subject or working on their behalf must be carefully considered. This section describes some of the key questions which must be answered before any sharing is undertaken.

5.2. This section applies irrespective of who is asking for or initiating the data sharing, including but not limited to: Commissioner Requests, transfers of information at the end of a contract, exchanges for companies producing systems for St Mungo's or requests from colleagues internal to St Mungo's.

5.3. Any attempt to share information must be able to identify the following:

(a) If St Mungo's is legally allowed to share information - can a clear legal basis be established?

(b) What is the sharing attempting to achieve? Any purpose described must be fair to the data subject and connected to the purposes for which St Mungo's gathered the information.

(c) To achieve the purpose, what must be shared? What is the minimum required for the sharing to be adequate, what might be excessive given the requirements?

(d) Who will require access to shared personal data? Both during and after the transfer, are these individuals trusted to handle the data and is their access proportionate?

(e) When should the data be shared? Will this be a regular transfer or a one off?

(f) How should it be shared? Are the mechanisms secure?

(g) How can St Mungo's check the sharing is achieving its objectives? Sharing that proves to be ineffective or insufficient should cease and data appropriately returned to St Mungo's control.

(h) What risks does the sharing pose? Especially where the data of children or sensitive data is involved what are the worst case scenarios, are all other answers proportionate to that risk?

(i) Could the objective be achieved without sharing the data or by anonymising it? In relation to 5.3 (c), can data be minimised to the extent it is no longer personal or is outside the scope of this guidance?

(j) Do privacy notices need to be updated? We must always be clear with data subjects how their information is used, does this sharing change those promises, are updates necessary?

(k) Will information be shared outside of the European Economic Area (EEA)? If so has Information Security (infosec@mungos.org) been informed and appropriate safeguards established.

5.4. St Mungo's must maintain auditable trails of disclosures, including:

(a) Ensuring staff can account for internal transfers and that privacy notices provided to clients or updates to them are an accurate description of transfers.

(b) That logs are kept for exceptional or ad hoc transfers outside of St Mungo's. These must be able to demonstrate adequate responses to all points from 5.3 in the case of a dispute or enquiry from the data subject or regulator.

(c) That written agreements are established for all systematic sharing outside of St Mungo's. These must provide adequate responses to all items from 5.3 and in additional make clear the division of responsibilities, identifies of and expectations between parties and the period of the agreement. Additional requirements depend on the nature of the relationship (see *J08 – Data Sharing Agreements* for further information).

5.5. Clarity on data sharing is an important element of St Mungo's practice and must be done so:

(a) We can keep privacy notices up to date and ensure we meet the data subject's right to be informed.

(b) We can respond to specific data subject queries effectively and quickly should they request information about how we have shared their data.

(c) Data subjects are aware of all organisations involved in processing their data, and St Mungo's can take action to inform individuals if any of our providers have a data breach.

(d) St Mungo's can maintain records of responsibilities that may be taken into consideration by our regulator, during any court proceedings or by a data subject following a breach of data protection principles.

(e) St Mungo's can quickly rescind any relationship with procured services or contracted processors who breach the terms of our agreements and make alternative arrangements with providers who have adequate safeguards.

Legal basis for sharing: When must the individual be informed?

5.6. Data sharing cannot be achieved without first establishing a legal basis, where that is unclear all processing, including sharing must halt until it is established. Guidance can be found in J04.

5.7. Each legal basis will determine the nature of the sharing. All sharing attempts will need to be considered against this. This section outlines some commonly used legal bases by St Mungo's and their implications for information sharing.

5.8. **Consent –** A key aspect is that consent must be informed and aware of how data will be processed. Sharing is a form of processing and you may only share information as you have received specific opt-in consent to do so. Internally this means clearly defining which St Mungo's functions will work with data. Externally this means listing who and why will also have access to data.

5.9. **Fulfilment of a contract** – Similar to above, it is only as valid as what parties to the contract have been informed of. Information may also be shared so long as it is specifically related to establishing or preparing a contract (e.g. requesting reference checks before signing employment contracts). However any sharing must unambiguously connect back to the contract and its purpose

5.10. **Crown Purpose / Public function**– Where we receive a contract from a government authority we may justify and sharing that assists with the government purpose that we are assisting with (e.g. referrals to support services to assist with delegated responsibility from the Homelessness Act 2002). All attempts under this header must consider the proportionality, risks to clients and 'need-to-know' basis very carefully before sharing, even when the request comes from the government agency who has provided the contract.

5.11. **Legitimate Purposes** – Any legitimate purpose must have been clearly presented to the data subject upon collecting the data. Data can be shared with any organisation so long as it falls within the boundaries of how the legitimate purpose was described. To avoid ambiguity all foreseeable sharing under legitimate purposes should be described to data subjects in advanced and any attempts to share outside carefully consider the balance of risks, proportionality and what an appropriate definition of 'need-to-know basis'.

5.12. All scenarios described in this section require transparent sharing that is visible to the data subject, either via privacy notices or by specifically informing the individual in advance of sharing. Individuals must be provided an ability to object, in some circumstances this will require clearly articulating to the individual why their information must be shared to meet other requirements. In circumstances such as consent, objection must lead to the immediate halt in any data sharing, in line with the individual's wishes.

Sharing without individual's knowledge

5.13. Some legal bases allow St Mungo's to share information without explicitly telling a client. Any attempt to do so must remain proportionate and have clear justification. Common scenarios are listed below:

5.14. **Vital Interests** – St Mungo's can share relevant information including health related information when an individual in imminent danger or life threatening circumstances. This sharing must always be with an appropriate authority (i.e. police / ambulance / fire brigade), and only includes sensitive data when the individual is specifically unable to give consent (e.g. incapacitated).

5.15. **Statutory purposes** – St Mungo's may not have to inform the individual of a disclosure where there disclosure was mandated or required by another law. Examples might include disclosure to police of suspected female genital mutilation (following the 2003 act), or

safeguarding referrals to a local authority where a vulnerable individual is at risk. Each example must consider carefully the requirements of the law, how that impacts on the need to inform the individual and what is reasonable given the circumstances.

5.16. **Criminal activity** – Where criminal activity is reasonably suspected, a clear detection or prevention of crime mandate has been expressed, information is required for the apprehension of a suspect, or information is requested for court proceedings – St Mungo's may choose to disclose information. Such disclosures would not require we inform the individual. This must also consider the policy *B18 Working with the Police and Enforcement Agents* and section 11 of this P&P.

5.17. **Taxation purposes** – Where a request from a legitimate taxation body has been presented to St Mungo's, St Mungo's may choose to comply or be compelled to share relevant information without informing the individual. Examples may include council tax or housing benefit investigations by local authorities or requests from HMRC.

5.18. **Legal confidence** – Where St Mungo's is seeking legal advice about a case, it may share relevant information with legal counsel to receive appropriate advice without informing the data subject.

5.19. All sharing without informing the individual must always have justifications, content, date, authorising manager and other information listed in section 5.3 should be logged either in the body of the text, in an attached letter or using a Data Sharing Request form (see supporting documents). At a later date this information may be provided to the data subject upon their request if the legal basis to withhold the information is no longer relevant.

Mergers, takeovers and acquisitions

5.20. In the event of any mergers, acquisitions of another organisation by St Mungo's or acquisition of St Mungo's by another organisation any personal data processed beyond that point must be consistent with the purpose for which it was gathered. The resulting organisation may continue to use the information but only as long as the purposes remain specifically consistent and in line with the established legal basis.

5.21. Under any circumstance the resulting organisation should take steps to inform data subjects of any organisational changes, where changes result in a significant difference in purposes the result should be treated as a data sharing, requiring updated privacy notices and consideration of if any processing remains fair and legal. Consent must be re-sought in any such case where it is the required legal basis.

Buying and selling databases

5.22. Any attempt to sell any personal information collected by St Mungo's must be approved by the executive team with the consultation of information security and only ever after review of what is legal given the purposes, legal bases and privacy information provided to a client. All attempts must additionally present with a full privacy impact assessment.

5.23. Any attempt to procure or buy information from a third party must receive the review of a manager of regional head level or equivalent and Information Security, or make reference to a previous information security decision on a similar category of data.

5.24. Any attempt to procure or buy information along with an entire system to dispense or manage the information must receive the approval of the head of IT in addition to information security and a regional head or equivalent manager.

Emergency response planning

5.25. Data sharing in situations of true emergency (life threatening situations, fire, and imminent crime) are all covered by exemptions to the data protection act. Such situations are likely to be characterised by a need to quickly respond, often without time to refer to policy or await the advice of Information Security. Managers must familiarise themselves with the guidance of all J policies in advance of emergencies. Where scenarios are likely managers should pre-plan for sharing and justifications, noting response in Privacy Impact Assessments.

6. Sharing data within St Mungo's

6.1. All St Mungo's staff, volunteers, locum, agency, temporary and other individuals who work in house for St Mungo's are bound by the Code of Conduct, acceptable IT use policy and information security policies and procedures. These collectively commit any staff member to uphold organisational standards to data security, privacy and confidentiality.

6.2. Whilst St Mungo's staff are connected via these shared standards and purpose, data sharing must still be considered within the organisation. By default personal information must be kept on a need to know basis, and information only ever shared with other staff where:

(a) The staff requesting the data have clearly articulated what data they will require,

(b) The staff requesting data have clearly stated about whom they will require data,

(c) The staff requesting data have clearly expressed how the data will be used,

(d) The usage has been reviewed and found to be consistent with the legal basis and purpose under which the information was gathered,

(e) The usage has been reviewed against privacy notices and ensures that the usage falls within the boundaries of assurances provided to the data subject. Where privacy notices are insufficient, managers or Information Asset Owners must consider if the data subject must be notified before sharing the data.

(f) The usage has been agreed to be relevant to the purposes, adequate and accurate enough to perform the task and a proportionate action, especially in consideration of a data subject's right to privacy.

(g) A mechanism has been agreed to securely transfer the data, either using IT approved channel internal (e.g. shared drive or internal St Mungo's email) or procured systems (e.g. mimecast). The staff sending data are responsible for ensuring the secure transfer and/or access to any data shared internally.

(h) The staff requesting the data have clearly established what will happen to the data after they have used it. If they retain a copy they themselves become responsible owners of the data and must be prepared to uphold data subject rights, manage the security of the data and ensure retention schedules are respected.

6.3. In addition, any internal sharing will apply the core principle that data must only be available on a need-to-know basis. Staff must consistently confirm if less can be shared to achieve common goals, and begin with default expectations of sharing the least personally identifying information required.

6.4. Data minimisation or need to know sharing must be considered not only by those who would release information, but also by staff who are making a request. Individuals should never ask for excessive information from other staff.

6.5. As part of GDPR implementation, staff should be prepared to challenge requests and ensure they can meet the standards of this section. This applies even where the sharing is long running or business critical. Where changes might elevate risk, Information Security should be alerted to help coordinate a response and explore alternatives.

Ad Hoc or Exceptional requests

6.6. Some requests for information are unforeseeable, either in response to changing circumstances or due to an emerging or emergency situation. These are known as ad hoc or exceptional request.

6.7. Core standards for ad hoc disclosures still apply. Staff sharing must consider all standards listed in 6.2 however unlike regular sharing, these may be established verbally and only logged if the data transferred is sensitive or regarding children.

6.8. This is not intended to be a barrier to work and instead is about making respect for client privacy and mitigating risk a default behaviour of staff, some examples of legitimate ad hoc sharing could be but are not limited to:

(a) Seeking advice of staff who had previously worked with a client, to establish how best to approach case management and support. This is entirely legitimate so long as information shared is kept strictly relevant to the client's support.

(b) An exchange of relevant risk information between St Mungo's services to mitigate risk to clients, staff or other individuals. Risk information should be specific and sufficient to identify the individual and react appropriately. Other information would fall outside this scope.

(c) Whistleblowing or safeguarding referrals to senior managers with sufficient information to establish the scope of seriousness or timelines for events.

(d) Sharing information with the business excellence team or senior managers for the purposes of resolving complaints, conducting audits, investigations, incidents or other mechanisms intended to provide oversight. Staff must always ensure requests for information and responses are proportionate to the task.

(e) Exchanges of data between the policy team and services to allow policy to coordinate a response with a Member of Parliament who is advocating on a client's behalf.

(f) Reporting breaches, or data subject rights requests to Information Security along with sufficient relevant information to receive accurate guidance and support.

6.9. Staff must always be prepared to challenge the justifications for ad hoc requests. Where answers are insufficient, Information Security (infosec@mungos.org) should be alerted to arbitrate and suggest alternatives.

Regular manual sharing requests

6.10. Some internal information sharing will be more established with greater regularity to help perform common functions.

6.11. Examples might include:

(a) An exchange of client files between services as part of a regular move on process,

(b) Exchange of staff information to process payroll with up-to-date addresses and bank details.

(c) Preparing and sharing information with archival services to retain long term copies,

6.12. The necessity of this data sharing should be subject to regular review, where less data can be shared it should be immediately removed.

6.13. Regular processing involving exchanges of sensitive personal data, the personal identifying data of children or large volumes of sensitive personal data should receive a high risk privacy impact assessment and have mitigating actions assigned. These must be reviewed by Information Security (infosec@mungos.org). Where possible secure system alternatives should be established.

6.14. Staff who receive a copy of information as a result of manual sharing request become directly responsible for its upkeep. They are responsible for its security, retention and any further data sharing in addition to all other applicable information security policies.

Systematic sharing via systems or pooled data

6.15. Much of St Mungo's work as an organisation is closely related. Pooling information internally, by making it available across multiple services or functions is often essential in achieving our goals and improving our services. This section sets standards for how such data might be pooled or shared via systems internally to provide these benefits whilst building in safeguards for privacy, strong security standards and meeting our legal requirements.

6.16. For the purposes of this section pooled data will refer to any information that is made accessible between services or functions of St Mungo's without resulting in copies being created that fall into the direct management of staff. It particularly includes shared systems or platforms that centrally provide information throughout the organisation. Some examples might include but are not limited to:

(a) **Central client systems** – Systems where we share support, risk, demographic and engagement data as clients move between our services.

(b) **HR systems or files** – Where data might be pooled between HR and finance teams to ensure appropriate payments are made.

(c) **Donor systems** – Where data might be pooled between fundraising teams working for different purposes or shared with other functions such as campaigns.

(d) **Directorate or inter-team shared drives** – Where limited quantities of personal data might be shared to help teams complete a common goal.

6.17. All pooled data must have assigned a single Information Asset Owner who takes responsibility for compliance of the information within. This IAO must be aware of or hold good records on:

(a) The names and contact details of all individuals who will have access the information

(b) The specific purposes for sharing or pooling data. Where these are multiple they must be specifically listed against staff or categories of staff that have been given access.

(c) A description of the categories of:

i. Data subjects whose information is available to staff, ii. Personal and sensitive personal data stored about these individuals.

(d) Where applicable, if access will be used to enable profiling.

(e) An indication of the legal basis for any access, including transfers or legal basis for any further onward sharing that will take place.

(f) Where possible, the envisaged time limits for erasure of the different categories of personal data.

(g) Any specific measures above and beyond adherence to St Mungo's policies that will be used to safeguard personal data via organisational or technical means.

6.18. Where large systems or complex pools of data feature different types of users, with different purposes and legal bases, the IAO must ensure that appropriate access controls are in place. Specifically:

(a) That the IAO has been provided with sufficient information (see 6.16) to accurately assign access.

(b) That any access is kept on a strictly data minimised and need-to-know basis.

(c) That all access is justifiable against the provided purpose and clearly connects to the legal basis for processing.

(d) That firm processes are in place to monitor, audit and revoke access for users should their purposes change or role come to an end are in place.

(e) That categories of access are regularly reviewed and spot checked against the requirements of 6.16.

6.19. Any Information Asset Owner must be able to meet all requirements in 6.16 and 6.17 before providing users with access. Users must be clearly informed of any information they must provide as a prerequisite to access and understand that they will not be provided access until the IAO is satisfied all conditions have been met.

6.20. Access controls, a requirement of all systems that use pooled data.

(a) Reduce the security risk profile, an appropriate organisational measure,

(b) Ensure that access is limited to those with a clear legal basis and requirement to use information,

(c) Ensure that information can only be used for the clear purposes that were articulated to the data subject on privacy notices.

(d) Ensuring the pool of accountable individual is kept to a minimum number to improve accountability and St Mungo's ability to quickly pinpoint where breaches occur.

6.21. Pooling information with external organisations will additionally require data sharing agreements that assign responsibilities and transparently document 6.17 and 6.18. See sections 7, 9 and 10 for further information.

Systematic sharing via copies of data

6.22. Where data is systematically shared by means that generate an additional copy (e.g. by emailing spreadsheets). The receiving party will gain full management responsibility for the data as an independent Information Asset Owner.

6.23. Staff should first exhaustively explore alternatives (making copies available only via shared drive folders, or on central systems with access controls) before making copies of data that must be independently managed.

6.24. Staff sending or copying data must additionally ensure:

(a) The receiving party has agreed to take over management of the information

(b) The source, legal basis, purposes and privacy notices documenting promises made to the data subject are clear to the receiving party.

(c) The receiving party specifically agrees to adhere to any technical and organisational security measures and retention periods assigned to the data.

7. Exceptional Sharing

7.1. Exception sharing is defined as anywhere that St Mungo's could not have foreseen a specific request for information, especially where there sharing is not systematic or is a 'one off'. Such sharing may be possible but must be subject to careful review. This section summarises some common cases for exceptional sharing.

7.2. Exceptional sharing must always have a clear legal basis. Generally information can only be shared when consistent with the legal basis under which it was collected. However a number of exemptions and alternative legal bases exist for exceptional and emergency circumstances. This section summarises some key areas with reference to other policy and information to ensure appropriate sharing and planning for these scenarios.

7.3. All exceptional disclosures must be carefully logged by managers responsible for authorising the disclosure. Logs must include the following information:

(a) A general summary of the information disclosed,

(b) Who the information was disclosed to,

(c) How any disclosure was justified,

(d) The date of the disclosure,

(e) The St Mungo's manager(s) who approved the disclosure.

7.4. Logs must only ever be used for the purposes described below and must be of sufficient quality to:

(a) Verify the lawfulness of the disclosure

(b) Assist with self-monitoring and internal audits on compliance,

(c) Ensure the integrity and security of personal data

(d) For the purposes of detecting criminal proceedings within St Mungo's

Police & Enforcement Requests

7.5. Information may be shared with police or enforcement agencies under its own legal basis which may supersede the reasons for which St Mungo's processes data.

7.6. Any request by police or enforcement agencies must always be in writing, clearly stating the purposes and legal bases of the request. It is common that these come formatted in a police Data Protection Act (DPA) form. This form is only a valid basis to share information if the legal basis clearly state that the information is required connected to:

(a) Detection or prevention of crime,

(b) To assist with the apprehension of a suspect,

(c) To assist with court proceedings,

(d) Any other administration of justice.

7.7. Only requests backed by a court order, order of law or secretary of state or invoking national security grounds require mandatory sharing. Police requests fall outside this bracket and so even upon receipt of a valid DPA managers may use their discretion, taking into account the rights to privacy and confidentiality when deciding what to disclose. Further guidance on specific scenarios can be found in *B18 – Working with the police*. Any cases that remain unclear should be referred to information security (infosec@mungos.org) before releasing information.

7.8. Neither data protection law nor St Mungo's policy and procedures should stand is the way of St Mungo's as an organisation or St Mungo's staff reporting a crime to emergency services. Such a report should be proportionate, but will not be regarded as data sharing for the purposes of this policy. After reporting, any attempts to interview, gain further information from the organisation or otherwise investigate should be treated in line with sections 11.5-11.8 and *B18 – Working with the police*.

Missing Persons

7.9. Whilst missing persons investigations are often conducted by police, being missing is not grounds for 'detection or prevention of crime' or 'apprehension of a suspect' and so may not use the justifications listed under 7.6. Missing persons requests from authorities should politely inform the requester that we cannot disclose any information, however if the individual is in current contact with staff or services they will pass on any message or encourage them to get in contact.

7.10. Any request from a family member in relation to a missing person should also not share their personal information without the prior consent of the data subject. A similar message to 7.9 should be provided.

7.11. The refusal to provide information must also extend to confirming or denying if an individual is known (currently or historically) to St Mungo's to prevent opportunistic and unjustified attempts to reveal information.

7.12. Where the level of concern for a missing individual is acute, relating to an imminent circumstance and St Mungo's is believed to hold key information it should be treated as a safeguarding request and elevated to the St Mungo's Safeguarding leads for decision.

7.13. This policy does not prevent staff reporting a client missing, either to other services or police. Information provided at that time should be proportionate to receiving assistance to locate the individual, and may be followed up with sufficient information to clarify the request. Further information beyond this point should not be provided and must be treated in line with 7.9-7.13. Where there is uncertainty, the case must be referred to information security (infosec@mungos.org).

Safeguarding

7.14. Data protection is the due care we provide to client's rights, undue caution must never be allowed to place clients at harm or block safeguarding referrals.

7.15. Any referral made directly about clients must contain proportionate information to fulfil St Mungo's safeguarding requirements. Where possible this action should be discussed with the individual.

7.16. If information is ever requested by a third party on the grounds of safeguarding, especially if St Mungo's has not initiated the safeguarding process through a referral, staff should ensure any request has been made in writing and is carefully considered. A relevant request must be proportionate to the risk and clearly justifiable on the grounds of a legitimate interest of St Mungo's, or where sensitive data exists a statutory responsibility.

Where any uncertainty exists concerns should be flagged to St Mungo's safeguarding leads and information security (infosec@mungos.org).

Statutorily (legal) requests

7.17. St Mungo's is also bound by a range of other UK laws and statutory requirements, some of which mandate disclosure in the case of certain circumstances. In each case where an external agency claims St Mungo's has a legal responsibility to disclose information managers must:

(a) Establish the existence of the law or statute in question,

(b) Reasonably verify the identity of the requester or recipient, ensuring they are a proper representative of the agency,

(c) Ensure the request has been made in writing to St Mungo's clearly stating the justification for disclosure.

(d) Be reasonably satisfied that the request is proportionate and balances the data subject's rights to privacy with the requirements proposed by other law. Where uncertainty exists information security (infosec@mungos.org) should be contacted for advice or to coordinate a legal response.

Commissioner requests

7.18. Commissioners may often make ad hoc requests for reports or information about a service or clients within. All services must refer to their contract which should state:

(a) The circumstances and any service level agreements for responding to commissioner requests.

(b) The legal basis for any information processed and the rights of access commissioners will have over that data.

7.19. Commissioner requests must still be subject to data sharing principles that ensure that their purpose is made clear, the use of data will be consistent with the legal basis and the level of access has been made clear to data subjects in advance.

7.20. Where St Mungo's is an independent data controller, operating a service with professional discretion, the rights of a commissioner to data may not be unlimited. St Mungo's must ensure any request cannot be satisfied with less identifying data or aggregate statistics (for the purposes of monitoring).

7.21. Services managers should ensure that contracts and data sharing agreements establish clear and firm boundaries about the sharing of data with commissioners. All data flows must be justifiable and legitimate by the standards of this policy and the GDPR and have a clear legal basis. Where requests from commissioners are regularly unclear in this area, service managers should alert their Regional Head or Regional Director and Information Security (infosec@mungos.org) to arrange a plan of proactive commissioner engagement around data protection standards.

Within St Mungo's

7.22. Exceptional requests may also come from within St Mungo's. Where the request comes from a team or function with a very different purpose (e.g. client services to policy, or client details for an HR investigation), staff must ensure that reasonable justification is provided and a legal basis is made clear by the requesting party. All staff to any level of seniority

must understand their legal basis for using any personally identifying information. Any requests made where this is not clear, especially where justifications and legal bases are uncertain, must be referred to information security (infosec@mungos.org) for review before disclosing information internally.

8. Sharing outside the European Economic Area

8.1. Information must not be transferred outside of the EEA, unless:

(a) It is for law enforcement purposes, or

(b) The transfer has been based on an 'adequacy decision' ruling approved by information security, or

(c) Appropriate safeguards exist that have been approved by information security, or

(d) Special circumstances have been otherwise approved by information security.

8.2. Information Security (infosec@mungos.org) must be informed of any international transfers outside the EEA to assign an appropriate grounds under 12.1, as necessary Information Security will also prepare relevant documentation and justification for ICO review or approval subject to the provisions of the GDPR and Data Protection Act 2018.

9. Anonymising & Pseudonymising data

Anonymous Data

9.1. Data that is properly anonymised can no longer be understood to be personally identifying, and as such is outside of the scope of requirements in much of this policy.

9.2. It must be impossible to identify any individual through the data by means of:

(a) Making reference to the data itself,

(b) Combing or cross referencing the data with publically available datasets (such public databases, social media or data disclosed into the public realm by a data subject).

(c) By combining or cross referencing the data with any information privately held, either in databases or in the form of prior knowledge of the data subject.

9.3. In practice, anonymised data is best understood as data that – should you yourself be included within it, accepting all the details you know about your own life and access you have to additional information about yourself – you would still be unable to identify yourself from the anonymised records.

9.4. In practice, anonymised data will most often be aggregate or percentage data that is impossible to turn back into specific individual records.

9.5. Due to the sophistication of modern data matching, even datasets that do not features names or IDs may be regarded as identifiable where the number of variables might shrink the pool of candidates to an unacceptably small number. For instance, listing the gender, ethnicity and nationality of an otherwise unidentified data subject may allow individuals to be identified with reference to other knowledge. Especially where an individual is a representative of a nationality that is uncommon within the data set or sample.

9.6. All data that was once personally identifying should be assumed not to be anonymous by default, and only classed otherwise with reference to clear justification and comparison to the ICO's anonymization code of conduct.

9.7. Anonymised or aggregate data should be the first choice for any data sharing internally or externally when services or teams are asked to share data. If anonymous data is not appropriate, teams should explore pseudonymous options only progressing on to more identifying formats of data in proportion and relevance to the justifications provided.

Pseudonymous Data

9.8. Pseudonymous data may be hypothetically re-identified. However it has been engineered to limit the risks of doing so or make the requirements for other information unreasonably large.

9.9. Most often pseudonymised data is used in datasets where the individuals personal data must be obscured, however individual characteristics must be identified. Examples might include:

(a) Internal gender-pay gap or disability monitoring. Where individual's circumstances must be calculated or assessed, but knowledge of the specific individual is irrelevant.

(b) Information that has been key-coded or hashed (obscured by a non-reversible secure method), where the ability to look up the value or variables to produce the hash are unavailable to recipients of the data.

(c) IP addresses or information on a user's browser or device when visiting St Mungo's website, that in and of itself does not reveal a user's name, but might be correlated with other data (e.g. login attempts) to establish identity.

9.10. The quality or level of pseudonymisation should be understood as the difficulty, likelihood or risk involved in any undertaking to re-anonymise the data. Staff disclosing data must always consider the range of tools available to any recipient and obscure the data to an appropriate level.

9.11. Pseudonymised data should be the default option for any data sharing that involves a requirement to assess individual circumstances without needing to actually identify the individual. Teams should only progress to sharing identifying data or sharing weakly pseudonymised data in proportion and relevance to the justifications provided by the requesting individual or organisation.

9.12. Pseudonymised data is a newly introduced concept under the GDPR and the Data Protection Act 2018. Any confusion about its application should be referred to Information Security (infosec@mungos.org) to receive specific advice and emerging examples of best practice.

10. Privacy by Design

10.1. St Mungo's systems will ensure:

(a) Data flows are easily represented within their system for each service or body of users who contribute or access information contained within.

(b) Data sharing agreements and other controller/processor agreements should be able to be represented under these systems with documents clearly associated and relevant metadata (information about the data held) available for reporting (i.e. expiry date).

(c) Systems will work towards robust processes for monitoring access controls and ensuring user's access are quickly revoked where appropriate.

(d) Ensure default options for exporting data encourage anonymised and appropriately pseudonymised options and that appropriate access controls or processes are in place to ensure oversight of exporting identifying details.

(e) Ensure simple logging systems are available to relevant managers to allow them to centrally log exceptional sharing.

10.2. St Mungo's information security, IT and system owners must work towards privacy by design to:

(a) Ensure transfer mechanisms for data are at all times robust, accessible and otherwise fit for purpose.

(b) Methods and means of monitoring access to St Mungo's systems as well as identifying usual traffic of behaviours that would merit further security investigation.

(c) Develop contingency and business continuity plans for denial of service attacks, threats of cybersecurity attacks or actual cyber security attacks to ensure data flows remain secure and accessible.

(d) Develop monitoring of attempts to inappropriately transfer data personal identifying data outside of the organisation and especially attempts to transfer or connect to servers or systems outside of the EEA.

10.3. All managers must work towards privacy by design by:

(a) Being aware of the standards of this policy and other information security policies.

(b) Engaging partners and commissioners in early and proactive conversations about legal basis, required sharing of data and required standards and documentation to prevent later surprises and frustration.

(c) Ensuring that attempts to pseudonymise data are appropriate to the level of risk and to call upon support of information security for guidance when uncertain.

(d) Ensure transfer mechanisms for data are at all times robust, accessible and otherwise fit for purpose.

11.Relevant procedures and documents

J08S01	Information Sharing Request Form
J08S02	Template Information Disclosure Log

ThamesReach

Privacy Notice

Thames Reach obtains, stores and uses your personal information when we provide you with a service. It is also necessary for us to show that we are complying with our legal obligations.

Our promise to you
Thames Reach will always abide by the law when collecting or using your information and will only use it for the purposes we collect it for. You can ask us to provide you with a copy of our privacy policy in a way that you can read.

Sometimes Thames Reach will need to contact other support agencies in order to provide you with a service who may ask for your consent to share information.

I understand Thames Reach staff may need to contact other support services on my behalf in order to provide me with a service. I understand that I am entitled to see any information kept about me and register my views about anything which I believe to be incorrect.

Name: …….

DOB: …….

Signature: ……..

Date: ……..