reconstruct

# Data Protection Procedure

# Data Protection Procedure

**Data Protection Policy Statement**
This policy and procedure details our expectations of all who work for or on behalf of the company. It includes guidance on safeguarding security, privacy and integrity of data that we receive, generate, use, retain, archive and destroy. It recognises our obligations to our staff, our customers and other stakeholders with whom we may work and share data where appropriate. It specifies how data subjects (individuals) may access data held about them by the company and it also references other company policies and guidance which provide more detailed information/procedural guidance on specific aspects of data management.

The Companies policy and procedure are based on the principles of the GDPR. These principles are outlined and explained in the body of this document.

A number of terms used in this document derive from the Data Protection Act 2018 and GDPR, where they have common meanings. These terms, and others annotated throughout this document by appended*, are explained in the glossary (Appendix 01).

**Appendices/References**
Appendices
Appendix 01 - Glossary of terms
Appendix 02 – Timescales and responsibilities for retention/destruction of data
Appendix 03 - Dealing with Subject Access Requests (SAR):
Appendix 03a – SAR Flowchart
Appendix 03b - SAR request form
Appendix 03c - SAR monitoring form

**References**

- Data Protection Act 2018 and related Guidance Notes (numerous) available from Information Commissioners Office (UK): www.ico.org.uk
- General Data Protection Regulation (Guidance) available from Information Commissioners Office (UK): www.ico.org.uk

**Scope**
**1.** This policy and guidance apply to all workers for and employees of the company who collect, produce, store, *process**, access or in any other way manage data that the company is responsible for in conducting its business. *Data**** is information which is stored electronically, on a computer or related device such as a compact disc or memory stick, within a networked system of computer terminals, or in any paper-based filing system. This explicitly includes *personal data****,*** which means data relating to any living individual who might be identifiable from that data and which may be factual (e.g. name, dob, postal/email address) or an opinion (e.g. a professional assessment of a member of staff or a service user); as well as other types of data commonly held by the company such as commercial tenders/contracts, company accounts/forecasts etc. which, whilst not necessarily identifying individuals, may for other considerations be regarded as sensitive or even confidential.

**2. It is required that all of the company's employees/workers operate according to this policy (and such other practice and procedural guidance that the company issues to specific groups on matters of data security and recording practice) at all times in performance of the company's business. Where any breach of policy may occur then**

**all share the obligation to ensure this is drawn to the attention of their relevant manager without delay so that remedial action may be applied.**

**Purpose**

**3.** The purpose of this policy is:

- to explain the importance of good data handling by all involved in conducting the company's business;
- to outline overarching messages of required practice, and;
- to signpost more specific company guidance where necessary.

The context includes the facts that individuals (and organisations) have rights in law as to how information about them is used and that such information must, with few exceptions, be made available to them on request. Also, that poor data handling can impair the company's performance and attract negative financial and reputational consequences.

**Background**

**4.** The principles outlined by the GDPR and EU Legislation may be summarised as follows:

**4.1 Fair and lawful processing of data –** this requires that *Data Controllers**clarify, at the point of collection of data, the purpose(s) for which it is to be used and with whom it may be shared or transferred/disclosed to. Conditions for lawful processing of *personal data**require that *data subjects** must either have consented to the processing, or that the processing is necessary for the legitimate interest of the *Data Controller* or the parties to whom the data is disclosed. Where *sensitive personal data** is processed, the explicit consent of the data subject will almost always be required.

In practice, consent from individuals to the limited use of the data they provide will be obtained at commencement of, and then during, the company's relationship with them; for example, through statements on application documentation, service provision contracts/agreements and so on, all of which will seek individuals' signed consents before company processing of their data. Where the information provided to us as the Data Processor, consent or justification of lawful grounds will have been sought by the Data Controller from the Data Subject(s).

**4.2 Processing of data for limited purposes –** this means that personal data must only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

In practice an example could be where an individual provides their data for the purpose of communication and the company later wishes to process their data for some other purpose (e.g. to offer them products or services from another company). In such an instance the individual's further consent would be required for the desired processing if this was not included in the original consent.

**4.3 Adequate, relevant and non-excessive processing of data** - this relates closely to b) above but emphasises the point that *personal data* should only be collected to the extent that it is required for the purpose(s) notified to the data subject. Any data which is **not** necessary for the stated purpose(s) should **not** be collected in the first place.

In practice this places a duty upon all Data Controllers and Processors (and hence all those working for the company) to ensure that data it seeks from customers, service users, staff etc. - in application forms, checklists and so on – are relevant for specific business purposes. It is **not** acceptable to seek and then retain information on the basis that it might possibly be useful in the future without a view of how it will be used.

**4.4 Accurate and up to date data –** this means that all reasonable care must be taken by the company to ensure that data it retains, particularly *personal data,* are accurate at the point of collection and updated appropriately through regular audit/review.

In practice personal data held by the company in its data-bases and individual files, whether paper or electronic, will be routinely updated by allocated Managers and administrators. Where factual data held may be discovered to be incorrect it may be replaced with correct data (e.g. names, DOB, current address etc.).

**4.5 Timely processing of data, which should not be kept for longer than is necessary** – data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

The principle here is that data should only be retained by the company for as long as it is needed for legitimate business reasons, and no longer. In relation to *personal data* the significance of this principle is considerable, since the longer it is kept the greater the risk to the integrity, confidentiality and security of the data.

In practice minimum timescales for the retention of different types of data are specified in various regulations and statutory guidance/codes of practice and where this is so, company policy is that data (paper and electronic) will be destroyed as soon as practicable after the minimum retention period has elapsed; unless documented otherwise, in the form of a specific company risk assessment by an appropriate senior manager. **A list of timescales for the retention/destruction of personal and other data typically maintained by the company is included as an appendix to this policy- appendix 2 refers**.

**4.6 Data must be processed in line with individuals' rights –** as well as establishing principles of good data protection practice for organisations which act as *Data Controllers,* EU legislation also establishes rights for data subjects which must be reflected in organisational practice. Broadly, these rights are:

- That data-subjects may request access to (including a copy of) any data held about them by the company – **see section of this policy entitled "dealing with subject access requests (SARS)".**
- That data-subjects may request their data should not be processed for "direct marketing" purposes, or in a way that causes "substantial, unwarranted damage or distress to themselves or anyone else" - **see sections of this policy entitled "suppression list" and privacy notice".**
- That data-subjects may request that data about them which they consider to be inaccurate is amended or destroyed – **see paragraph 4.4 above and section entitled "advice for dealing with complex issues".**

- That data subjects may object to, and expect review of, any decisions which affect them which may be made solely by automated process (without human involvement).
- That data-subjects have the right to approach the relevant *Information Commissioner* (UK) to make representations about any Data Controller's policy and practice, and/or the right to seek legal redress and/or compensation in respect of wrongful organisational practice – **see references section of this policy which cites sources of useful information.**

**4.7 Data Security –** this principle is fundamental to good data protection practice, pervades all the other principles cited. It is the responsibility of everyone working for the company to maintain the security of all personal data from the point of collection to the point of destruction. This means following the instructions, as will inevitably be updated from time to time, in relation to networked computer systems, email, paper-based filing systems, dealing with customers over the telephone and so on.

Specific company policies that refer include: ***Electronic Communications Policy and Guidance***; ***Use of Mobile Phones and Similar Devices;*** **and current practice guidance on recording and archiving in the company's Operational Standards and Procedures manuals.**

Maintaining data security means guaranteeing the confidentiality, integrity and availability of personal data (and such other data as may be commercially sensitive for the company). That is:

- **Confidentiality –** only people who are authorised to use the data should be able to access it. This is often referred to as "need to know" and is the basis on which access to personal data is limited by company/ specific staff groups throughout the company.
- **Integrity –** means taking care to assure the suitability and accuracy of data for the purpose(s) for which it is processed
- **Availability –** means that authorised users should be able to access data for authorised purposes and, for example, is a key reason why electronically held personal data should be stored on the server-based system rather than on individual PCs.

Some general company expectations on maintaining data security include:

- **Physical entry controls –** ensuring restrictions of access to designated parts of offices and reporting unauthorised visitors
- **Lockable desks/cupboards –** to ensure that any hard copy personal data or commercially sensitive data is kept secure and a "clear desk policy" is maintained
- **Careful archiving and disposal –** personal data must be archived and destroyed in keeping with the timescales applicable (appendix 2) by the responsible managers. This applies to electronic and paper based data. Paper documents must be shredded. Data storage on removable media – discs/cds/memory sticks- is actively discouraged unless absolutely necessary, but where exceptionally used the media must be physically destroyed when no longer needed; the IT department can advise on the safe use and data removal from memory sticks. Old PCs/laptops must be returned to the company IT team for re-imaging. Automated reports will alert staff when to archive/delete server –based data.
- **Screen security –** all computer users must ensure machines are not left "open to view" to non-authorised persons.
- **Email –** all users must take care to properly direct and where necessary password-protect messages/attachments and avoid forwarding unnecessary email trails which risk unintentional disclosure of personal data of individuals within the trail. Company policy is that all attachments to e-mails which include any sensitive and/or confidential

personal data must be password protected by the sender or sent using secure online portals such as Egress- **this applies to emails sent within and out with the company's secure system.**

- **Passwords and log-in details –** all users must keep private their log-in details for company electronic systems and only access systems using their own details as these will often determine levels of authorised access to data. Passwords for company PCs and mobile devices must be frequently changed by individual users.
- **Telephones –** checking caller identities, referring difficult enquirers to line managers and ensuring that personal data are not disclosed inappropriately.
- **Confidentiality awareness –** never discuss sensitive company business or personal data of service users with non-authorised staff, or outside of the workplace, whether face to face or via any electronic media. Do not retain company confidential or personal data on company laptops for longer than absolutely necessary (store on company server-based system) and under no circumstances may such data be transferred onto non-company issued machines or systems. Unless absolutely necessary and with appropriate management authorisation, do not convey paper-based confidential or personal data out of your usual office-base.

4.8 **Transfer of data beyond the European Economic Area –** the final data protection principle requires that EEA data controllers and processors should ensure that personal data are not transferred to non-EEA countries unless adequate levels of protection of the rights and freedoms of data subjects can be assured.

In practice it is for the company to make its own assessments in this regard and reference to guidance available from the Information Commissioner (UK) and/or to seek advice from the company solicitor first. Generally, it is understood that interpretation of "transfer of data" does not extend to include electronic data in transit from one country to another; rather, it only relates to the country of actual destination. Issues of **necessity** for the transfer of data in the interests of data subjects, the **public interest** and the **consent of individuals** to personal data transfer will always be at the heart of individual decision making concerning international transfers.

4.9 The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

**Procedure and Practice**

**5. Awareness, training and advice/reporting on complex issues**

5.1 All staff are required to understand and respect the principles of good data protection/data handling practice in processing company data for which they may share responsibility in their day to day duties. It is the responsibility of managers to ensure staff/worker competence through induction, training and supervision. All staff that have any role in processing personal data and/or dealing with customers/service users must read this policy and discuss any queries, in the first instance, with their respective line managers.

5.2 Every 2 years data protection training will be undertaken by staff via the Information Commissioner Office website training videos or internal produced training material based on this. The company should ensure the availability of sufficient operational managers who have attended training so that they may act as a local first points of reference for any local data protection practice or procedural queries that may arise; particularly, but not exclusively, in relation to Subject Access Requests.

5.3 Officers within company act as data protection advisers for the company and maintain and monitor those aspects of the company Risk Register specific to data protection issues and

SARs and should be contacted for advice and assistance on complex issues.
**Any** breach of data protection legislation/good practice –e.g. loss or wrongful disclosure of personal data - must be notified to the Operations Manager and/or Office Manager, for escalation to the Data Protection Officer by telephone and then followed up in writing with the appropriate risk assessment.

The Data Protection Officer in conjunction with the Operations Manager will then provide follow up advice and instructions as to action to be taken and retain an appropriate audit-trail, including a **register of all business risks and all SARs** received/responded to. Following any breach an immediate action plan will be put in place to ensure prompt investigation and communication with affected parties such as data subjects, relevant local authority or other service commissioners, and relevant public offices (e.g. ICO). Lessons learned from such events will be used to enhance staff awareness and improve practice and company systems; where appropriate disciplinary action may be taken.

**Dealing with Subject Access Requests (SARS)**
6.1 Individual *data subjects*, whether employees/other workers, customers/service users, and so on, are entitled under EU law to see and receive, where requested, copy in "permanent form" of *personal data* that we may hold about them. This places clear obligation on the company and all staff responsible for data maintenance and/or archiving to ensure that such data are maintained according to company protocols and practice guidance (e.g. regarding data-base entries/security, case recording, and data retention/cleansing/disposal) and that data can be readily located and retrieved whenever it may be needed.

6.2 The company have a designated SAR Holder (Operations Manager) to whom all SAR received should be directed to in the first instance. The SAR Holder will then notify the Data Protection Officer accordingly and disseminate the processing and management of any SAR requests to appropriately trained members of the management team.

Data Subjects have the following rights concerning their personal information:

- **SAR 1: RIGHT BE INFORMED** – Keep data subjects informed of the recording which is made about them, wherever possible as it is made - e.g. staff, customers and service users. This information should be covered either contractually or via the company's privacy notice. If we are the Data Processor, the Data Controller should have notified the data subject accordingly regarding this, supported by our Privacy Notice, policies and procedures in relation to this. A culture of openness is likely to reduce the demand for time-consuming retrospective data disclosure.
- **SAR 2: RIGHT OF ACCESS** - The right of access to personal data relates to the specific *data subject* – i.e. an individual does not generally have the right of access to personal data about other individuals who may be referred to in the primary data subject's case records etc. Whilst there are some circumstances in which the disclosure of personal data to the data subject may be legitimately withheld (see appendix 3d) it is safer to assume that disclosure upon request will be the usual default position.
- **SAR 3: RIGHT TO RECTIFICATION** – The right to have any incorrect or out of date information regarding the data subject to be updated throughout our records where appropriate. Please note that there will be instances where we are not the Data Controllers and as such will need to liaise with them accordingly concerning this before taking any action.
- **SAR 4: RIGHT TO ERASURE –** the right to have any personal data held on them erased from our system. Please note that there will instances where are unable to do

so due to a number of reasons which may include; company policy regarding specified retention periods, lawful basis for processing/retaining the information, relevant legislation and guidance. Please ensure that these are reviewed in the first instance and where necessary advice sought from the SAR Holder/DPO/ICO before taking action.

- **SAR 5: RIGHT TO RESTRICT PROCESSING** – the right for the data subject to request for how their data is processed. Please note that there will instances where are unable to do so due to a number of reasons which may include; company policy regarding specified retention periods, lawful basis for processing/retaining the information, relevant legislation and guidance. Please ensure that these are reviewed in the first instance and where necessary advice sought from the SAR Holder/DPO/ICO before taking action.
- **SAR 6: RIGHT TO DATA PORTABILITY** – the right for their data we hold to be transferred to another agency to process. Please note that there will instances where are unable to do so due to a number of reasons which may include; company policy regarding specified retention periods, lawful basis for processing/retaining the information, relevant legislation and guidance. Please ensure that these are reviewed in the first instance and where necessary advice sought from the SAR Holder/DPO/ICO before taking action.
- **SAR 7**: **RIGHT TO OBJECT –** the right to object to their data being processed. Please note that there will be instances where the company are not Data Controllers and as such discussions may need to be held with them before any action taken. Additionally there may be contractual or legal bases on which we are required to process the data. Guidance should be sought where uncertain concerning this.

Accordingly, it follows from the above that all recording of personal data (note, this includes professional opinion) should be undertaken with due professional care e.g. by ensuring accuracy and distinction between fact and opinion, avoiding subjectivity or over-long recording, clarifying where specific data may carry a condition of legal professional privilege or expectation of confidentiality, and maintaining individual-discrete files/records rather than group-based records.

The data subject may in the first instance be referred to the company's Privacy Notice which is on the website.

Where a data subject requests access to their personal data this will be responded to in one of two ways:

- Response to a "**routine enquiry**" - for example, a current or ex-employee with a simple and reasonable request to be reminded of an item of their personal data they know the company holds and may even have previously received from the company (my NI no., my last payslip, my last performance appraisal etc.) should be given the information by the relevant manager without any further formal process.
- Response through reference to the **Subject Access Request** (SAR) procedure – this will apply where the request is for extensive and possibly sensitive information where there may be complicated issues about separating out personal data about third parties and issues of confidentiality, and/or where extensive searches of data bases or archives are necessary to retrieve the data requested.

6.3 Responses to **routine enquiries** should be dealt with as promptly as possible and noted on the running record of the relevant data subject's company file/data base. Responses to formal **Subject Access Requests must be dealt with through the company's SAR procedure which is set out in the appendices to this policy:**

- Appendix 3a - Responding to SARs, flowchart
- Appendix 3b - SAR request form
- Appendix 3c – SAR monitoring proforma

The SAR procedure will be managed by the SAR Holder (Operations Manager) or a relevant manager who should take advice as necessary from one of the nominated Data Protection Advisers and DPO within the company. Monitoring records of all SARs must be kept as per the instructions in the above appendices. It is the responsibility of company senior managers/departmental heads of service to ensure that they sustain sufficient locally nominated managers who have received the necessary company data protection training.

6.4 It is important to recognise that:

- Data protection legislation, the GDPR and associated good practice relates to data that may be held on paper **and /or** electronically. As such, those dealing with SARs will need to be able to identify and interrogate all relevant company recording media that may hold an individual's personal data. Inevitably this will in some instances involve accessing assistance from staff with specific technical expertise (e.g. IT) in relation to relevant electronic systems/databases; and in others will require liaison with designated administrative managers regarding recall of closed paper records from archives. Both of these considerations will need to be factored in for meeting the **30 (calendar) days** indicative timescale which generally applies to all SARs, alongside other potentially time-consuming tasks such as "vetting" information to be disclosed for third-party content, and/or consent from third-party providers of personal data which the company records might include.

- With regard to identifying personal data held on electronic systems/databases it is important to stress that care must be taken if it is decided to supervise a data-subject's viewing of their information on screen. Specifically, individuals must not be inadvertently allowed access to other people's personal data (many records will contain references to third parties and will therefore require the member of staff dealing with the SAR to view what might be seen by the data subject before they see it) and it will never be appropriate to afford a data subject unsupervised access to company systems. In most instances it is likely that individuals will require hard copy of personal data they request.

**Dealing with requests for access to commercially sensitive data (not *personal data*) – Freedom of Information Acts (FOIA: 2000 (England, Wales, NI), 2002 (Scotland)**

7.1 The FOIA provides for access to information held by **public** authorities. The aim of the FOIA is to promote transparency and improve public confidence and as a result authorities are obliged to publish certain information. More importantly, the FOIA also entitles members of the public to request information held by public authorities. The FOIA covers any recorded information held by a public authority in England, Wales and Northern Ireland. Information held by Scottish public authorities is covered by the Freedom of Information (Scotland) Act 2002 which has similar provisions.

7.2 Although the FOIA does **not** concern personal data, it is relevant to the company both in terms of the information supplied to public authorities upon submission of tenders by the Tender Unit and any later request for that information from a member of the public.

7.3 There are various exemptions available under the FOIA, the most relevant to the company being information which is confidential or information which is deemed commercially sensitive. Upon submission of any tender, our pricing or any financial information submitted by the Tender is deemed commercially sensitive and, where there is an opportunity to do so, the authority is informed of this.

7.4 Every contract entered into with a public authority will contain an obligation on the company to abide by certain timescales in relation to FOIA requests. If a request for information is received from a member of the public, it must be forwarded to the relevant authority upon receipt as contractual provisions can contain an obligation to forward requests in as little as 2 working days. In the event an authority receives a request concerning information relating to us, it will normally contact us requesting views as to its release. If a request is received and there is any doubt as to the course of action to take, please contact the Commercial (Risk) Solicitor who will assist you. **In no circumstances should a request be responded to directly.**

**Suppression List**

8.1 In keeping with data protection principles previously cited (particularly 4.2 and 4.6) the company has developed a *suppression list** to record those individuals who do not wish to receive direct marketing materials. The list contains sufficient details to enable an individual to be identified without providing full names and addresses and exceeds the requirements of UK legislation by allowing full preferences of individuals to be recorded. For example, should a customer choose not to receive all marketing materials for us, yet is content to receive marketing materials electronically, this preference is recorded and must be enacted.

**Privacy Notice**

9.1 Data protection legislation and principles (particularly 4.1 and 4.6) require that individuals are kept informed as to the collection and processing of their personal data. A *privacy notice** is designed to ensure individuals know how information collected about them will be used and the likely implications of that use. It also details whether or not that information will be shared and who that information will be shared with, which is particularly important when dealing with sensitive personal data.

The privacy notice also highlights “special categories” of personal information, which requires a higher level of protection because it is of a more sensitive nature. The special categories of personal information comprise information about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data. We may collect sensitive personal information throughout the period of our working relationship as a result of statutory or contractual requirements.

The website has a separate privacy notice accessible via the home page under “Privacy Statement” which gives the above details in full, together with details of how an individual can access a copy of the data the company may have collected about her/him (see also section 6 of this policy).

**Recording practice and document control**

10.1 All data we hold is stored electronically and any paper documents are securely destroyed.

10.2 **All** managers and staff must own and exercise personal responsibility for good data management regarding records that relate to their job roles. This means:

- Understanding **what** files/data bases they are required to contribute to and maintain
- Understanding **why** they are required to maintain these records-in terms of the purpose(s) they serve
- Understanding **How** they must maintain these records- for example whether electronically or otherwise, by what specific operating rules (e.g. company data entry protocols, specific regulatory/good practice considerations)
- Understanding **who** may have interest in and/or responsibility for these records - e.g., who "needs to know" the content, who may have a right of access (and who doesn't), who is responsible for auditing/archiving.

10.3 Detailed instructions and advice on recording practice and document control are available from a range of sources which include:

- Company-specific **Operational Standards and Procedures**
- Access to technical/professional expertise from **managers with specific roles and functions** at local and company levels – e.g. Company Secretary, Quality Assurance Managers, Risk Department, Quality and Performance Managers, IT Department, Business Partners (HR and Learning and Development), local Administration Managers etc.

10.4 With specific regard to **data retention and destruction,** we operate to the data protection principle outlined at Para 4.5. That is, data will be retained for as long as necessary for operational effectiveness and to reflect specific regulations, but not for longer than these drivers demand. A list of some of the key timescales for retention of different kinds of information is included at **appendix 2**. Good housekeeping demands that these must be adhered to if systems are not to be overloaded and archives are not to become burdensome and/or their security compromised. As per paragraph 10.2 above **all managers must ensure that data/files for which they have responsibility:**

- Are maintained correctly and up to date in accordance with company and regulatory requirements
- Wherever possible, data subjects should be encouraged to contribute to and be aware of what is recorded about them
- Are not accessible to those who do not have good reason to see them
- Are clear as to the degree of confidentiality that applies, including the limitations of any implied guarantee of confidentiality
- Are consigned to the relevant physical (hard copy) or virtual (electronic) archives when no longer active, together with the necessary record/prompts to ensure that they are proactively retrieved for destruction when their retention period expires - for electronic archives this will be achieved through automated systems' programmes, but for hard copy archives, deposited records (what, where, when deposited/to be retrieved) must be maintained systematically by responsible administration managers.

10.5 A number of documents which are essential for different aspects of our business are required to bear signatures and dates to assure their authenticity. This reflects the possibilities that they may need to relied upon at some future date, perhaps in the context of clarifying accountability, dispute resolution or presentation in a legal arena. These include, for example:

- **Contract related documents** – service level contracts with commissioning bodies, individual placement contracts/funding agreements

- **Staffing related documents** – contracts of employment, appraisals and supervision agreements/notes, confidentiality undertakings, expenses claims
- **Service User related documents** – Form F reports, consent forms for statutory checks, foster care agreements and undertakings, carer supervision agreements/records.

10.6 Such documents (and others not mentioned in the list of examples) require careful attention and management from those responsible for their completion and retention. This arises particularly where such documents are maintained electronically on systems which may not carry sufficiently flexible options for robust authentication of electronic signatures from necessary individuals. Departmental managers will need to establish appropriate protocols for specific scenarios and communicate these to relevant staff to ensure consistent practice. The advice from a relevant Senior Manager or Commercial (Risk) Solicitor should be sought regarding specific instances but the general default position will be that such documents must be printed, signed/dated, scanned and then uploaded to the relevant system.

**Review**

**11.** This policy will be kept under constant review by the Operations Manager and other relevant managers and updated as necessary in the light of operational experience. There will be a minimum annual review in the absence of changes prior to that (details for this will be detailed on the Data Protection Policy). Any changes will be notified through subsequent information bulletins to staff and the policy library.

**Appendices**

Appendix 01 - Glossary of terms
Appendix 02 – Timescales and responsibilities for retention/destruction of data
Appendix 03 - Dealing with Subject Access Requests (SAR):
Appendix 03a – SAR Flowchart
Appendix 03b - SAR request form
Appendix 03c - SAR monitoring form

## VERSION CONTROL

| | | | Document Owner | Reconstruct Ltd |
|---|---|---|---|---|
| | | | Status | Active |
| | | | Next Review | 30/09/2024 |
| Version | Revision Date | Section Revised | Person undertaking Revision | Reason for Revision |
| V_2 | 11/10/23 | All | AD | Review of policy, rebranding, and implemented version control mechanism opposed to having just date for next review |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |