DATA PROTECTION AND ACCESS TO RECORDS POLICY

For the latest version of this policy please refer to the electronic location below

Policy Number	JL/Group/IG02
Version Number	01
Purpose	This policy: • Aims to ensure that Jane Lewis complies with data protection law; • Protects the rights of people in receipt of care, colleagues and other people who have a relationship with Jane Lewis; • Is open and honest about how Jane Lewis processes personal data; and • Manages data protection risks.
Scope	This policy applies to: • All colleagues across Jane Lewis. • All personal data collected and used by Jane Lewis regardless of format. It also covers any personal data generated by third parties acting as a data processor for Jane Lewis.
Policy Owner	Kevin Monteith, Director of Risk and Governance & DPO
Policy Ratified	Kevin Monteith, Director of Risk and Governance & DPO on 26/02/2024
Policy Signed Off	Katy Lineker, Chief Financial Officer on 03/03/2024
Date Issued	07/03/2024
Date for Review	06/03/2027
Electronic Location (EL)	Intranet/Sharepoint and ECHO

DATA PROTECTION AND ACCESS TO RECORDS POLICY

1 INTRODUCTION

1.1 In order to provide services, Jane Lewis needs to gather and use personal data about individuals, including people in receipt of care, colleagues, suppliers and other people who have a relationship with Jane Lewis

1.2 This policy sets out the steps that Jane Lewis will take to comply with data protection legislation when processing personal data and should be read along with Guidance for Requests for Access to Records (**JL/Group/IG/G-01**) and the Standard Operating Procedure Handling Subject Access Requests (SARs) (**SOP047**).

2 DEFINITIONS

2.1 **Personal Data** means any data relating to an identified or identifiable living individual. Identifiable living individual means a living individual who can be identified, directly or indirectly, in particular by reference to:

(a) An identifier such as a name, an identification number, location data or an online identifier; or

(b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

2.2 **Data Controller** means a person or organisation which alone, or jointly with others, determines the purposes and means of the processing of personal data.

2.3 **Data Processing Activity** means any activity that involves the processing of personal data. Processing means carrying out any operation or set of operations on the personal data.

2.4 **Data Processor** means a person or organisation which processes personal data on behalf of a data controller.

2.5 **Data Protection Impact Assessment** is a process to help identify and minimise the data protection risk of a data processing activity.

2.6 **Data Subject** means the person to whom personal data relate.

2.7 **Data Subjects' Rights** means the right of access by the data subject, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability, the right to object and rights in relation to automated decision-making.

2.8 **The Information Commissioner's Office (ICO)** is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

2.9 **A Privacy Notice** is a verbal or written statement that informs people about the way in which their personal data are used.

3 RESPONSIBILITIES

3.1 **Operational Risk Management**
Risk management responsibility is delegated through the line management structure from CEO to Managing Directors with Hospital Directors/Service Managers having day to day responsibility for risk control measures within their areas.

3.2 Operational management is supported by a range of corporate services with underpinning internal controls, which collectively constitute the company's governance and assurance processes.

3.3 **Information Governance**
The key roles and responsibilities for information governance, which includes data protection, are set out in the Jane Lewis Information Governance Policy.

3.4 **Line Managers**
In addition, all line managers are responsible for ensuring that colleagues managed by them are:

(a) Given sufficient time away from their other duties to undertake their annual information governance eLearning course.
(b) Supported to undertake additional data protection training where their role requires it.
(c) Supported to meet their data protection obligations, and
(d) Encouraged to report information security incidents and any issues that have the potential to result in an information security incident.

3.5 **Colleagues**
All colleagues are responsible for:

(a) Completion of the mandatory information governance eLearning course.
(b) Identifying any additional data protection training needs with the support of their line manager.
(c) Understanding, and adhering to, any policies, standards and procedures for data protection.
(d) Reporting information security incidents, and
(e) Reporting any issues that have the potential to result in an information security incident.

4 COLLEAGUE TRAINING AND AWARENESS

4.1 Contracts of employment will contain provisions for data protection and confidentiality. Such clauses will include information about the consequence of non-compliance.

4.2 All Jane Lewis colleagues will be required to complete information governance eLearning, which includes modules relating to data protection, followed by refresher eLearning every three years.

4.3 Jane Lewis will aim for 85% of colleagues to have completed information governance eLearning, recognising that a 15% tolerance for non-compliance allows for colleagues who are not at work for reasons such as long-term illness or maternity/paternity leave.

4.4 Line managers will be responsible for supporting any colleagues that they manage to identify and fulfil any additional data protection training needs.

4.5 The training needs of colleagues with specific data protection roles and responsibilities will be outlined in the applicable documented role description.

5 DATA PROTECTION OFFICER

5.1 Jane Lewis will designate a Data Protection Officer with the necessary expertise and influence to carry out these responsibilities. The Data Protection Officer's responsibilities are set out in the JANE LEWIS Information Governance Policy.

6 RECORD OF PROCESSING ACTIVITIES

6.1 Jane Lewis will maintain an up-to-date record of data processing activities that involve personal data.

6.2 The record of data processing activities will include the lawful basis for processing the personal data.

7 DATA PROTECTION BY DESIGN AND BY DEFAULT

7.1 At the point of designing new data processing activities, or redesigning existing data processing activities, Jane Lewis will integrate appropriate technical and organisational measures to protect the personal data and the rights of the data subject.

7.2 Suitable measures will be identified through completion of a Data Protection Impact Assessment and may include such measures as data minimisation or the application of anonymisation techniques.

7.3 Where a data processing activity is assessed as presenting a high risk to the rights and freedoms of data subjects and Jane Lewis is unable to implement suitable measures to reduce the risk, the Data Protection Officer will refer the Data Protection Impact Assessment to the ICO.

8 TRANSPARENCY

8.1 Where consent is the most appropriate lawful basis for a data processing activity, the request for consent will be:

(a) Prominent and separate from any other terms and conditions.

(b) Based on a positive opt-in – we will not use pre-ticked boxes or any other form of default consent, and

(c) Presented in clear, plain language that is easy to understand.

8.2 Any request for consent will explain to the data subject that consent can be withdrawn at any time without detriment.

8.3 Where there are concerns that the data subject may lack the capacity to consent to a data processing activity, the provisions of the Mental Capacity Act 2005 (in England and Wales), the Adults with Incapacity (Scotland) Act 2000 (in Scotland) will apply.

8.4 Where an alternative lawful basis is identified for the data processing activity, consent will not be sought from the data subject, but a privacy notice will be provided. See Section 14 Associated Documents for details and links to Jane Lewis Data Privacy Notices.

8.5 A privacy notice will be provided at the point of data collection where personal data are provided directly by the data subject. Where personal data are provided by a third party, a privacy notice will be provided as soon as possible and, in any event, within one month.

8.6 Privacy notices will be concise, transparent, intelligible, easily accessible and written in clear and plain language taking into account the needs of the data subjects.

8.7 A bespoke privacy notice will not be provided where it would prove impossible or involve disproportionate effort to do so. In such circumstances, generic privacy information will be made reasonably accessible in hard copy or online.

9 DATA SUBJECTS' RIGHTS

9.1 Procedures and supporting guidance materials will be developed and implemented to ensure that data subjects' requests to exercise their rights are handled in accordance with data protection legislation.

9.2 Information will be made available to data subjects informing them of their rights and the way in which they can exercise them.

10 SECURITY

10.1 Jane Lewis will implement appropriate technical and organisational measures to protect the personal data and the rights of the data subject. Such measures will take account of risks to the rights and freedoms of data subjects, the nature, scope, context and purposes of the processing, the technology available (where relevant) and the costs of implementation.

10.2 Personal data will only be transferred to a country outside of the European Economic Area (EEA) in the following circumstances:

(a) The country or international organisation is identified by the European Commission as providing an appropriate level of protection.

(b) The country or organisation has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are in place.

(c) The processing is undertaken by a group of undertakings, or a group of enterprises engaged in a joint economic activity, and is subject to binding corporate rules for its international transfers - such rules will include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(d) The data subject has explicitly consented to the proposed transfer after having been informed of the possible risks, or
(e) Any other derogation set out in Article 49 of the GDPR applies.

11 INFORMATION SECURITY INCIDENTS

11.1 All information security incidents and data breaches must be reported on Datix.

11.2 The Group DPO will notify the ICO where required.

11.3 Information security incidents involving personal data will be notified to the data subject without undue delay unless one of the following is applicable:
(a) Technical and organisational measures, such as encryption, were applied to the personal data affected.
(b) Upon discovery of the incident, JANE LEWIS has been able to implement measures which ensure that risks to the rights and freedoms of the data subject are no longer likely to materialise, or
(c) Informing individual data subjects would involve disproportionate effort, in which case, a public communication or similar will be considered.

11.4 Notification of an incident to the data subject will include information on how the data subject can make a complaint to the ICO.

11.5 Information security incidents will be fully investigated to determine their cause. Actions to mitigate risks and to reduce the likelihood of reoccurrence will be identified during the investigation and implemented accordingly.

11.6 JANE LEWIS will cooperate fully with the ICO in the event of an information security incident.

12 EQUALITY IMPACT STATEMENT

12.1 This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any employee or applicant and it helps to promote equality in our services.

13 REFERENCES

13.1 **Legislation**
Data Protection Act 2018 (as amended)

13.2 **Guidance**
Guidance produced by the ICO is available at www.ico.org.uk

14 DOCUMENT VERSION HISTORY

Version	Description of Revision	Date of Revision
01	New Groupwide policy	07/03/2024