Privacy Notice

Data Subject Rights Procedure

1. Introduction

This data subject rights procedure (this "procedure") sets out the procedure to be followed by all Sister Pictures Limited ("**Sister**") employees, workers and contractors ("personnel/you/your") in the event of receipt of a data subject rights request. This procedure must be read together with the Sister Data Protection Policy.

This is a Sister procedure and applies to all personnel. It has been prepared with due regard to the Data Protection Act 2018 and General Data Protection Regulation ("GDPR"), which applies from 25th May 2018, and which grants rights to data subjects in the UK and EU. This procedure is to be followed when a data subject in the UK or EU exercises one or more of their rights.

It is important to facilitate the exercise of data subject rights in the manner required by the law. The purpose of this procedure is to set out what is required of Sister in the event that a data subject rights request (a "rights request") is received from a data subject in the UK or EU.

A data subject can make a rights request at any time and through any means of communication. It is therefore important that all Sister employees are aware of the rights available to data subjects in the UK or EU and the steps to take upon receipt of a rights request from a data subject in the UK or EU.

You must follow this procedure when responding to a rights request from a data subject in the UK or EU. Any failure to do so may result in disciplinary action.

2. Data Subject Rights

Data subjects in the UK or EU have the following rights regarding personal data processing and the data that is collected and held about them:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure (also known as the 'right to be forgotten');
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights with respect to automated decision-making and profiling.

All requests by data subjects in the UK or EU to exercise their rights must be facilitated as set out in this procedure.

3. Steps to Follow

The following steps and actions are to be taken in the order shown upon receipt of a rights request:

No.	Step	Action
1	A data subject submits a rights request. This can be by email, by letter, telephone or in person. It may be received by any Sister employee or worker.	Communicate receipt of a request without delay, by sending an email with details of the request to the Sister Data Protection Officer at dpolondon@sister.net
2.	Use all reasonable efforts to verify the identity of the data subject.	If the data subject is known to Sister and their identity is not in doubt, it will not be necessary to

		perform any additional verification checks. If further information is required, the Data Subject Rights Request Form template at Schedule 1 is to be used. This form can be amended as appropriate with the authorisation of the Sister Data Protection Officer.
3.	Evaluate the data subject request to determine how to respond.	Sister will confirm receipt of the request and verification of the data subject's identity. The Sister Data Protection Officer will assess the request and the information provided by the data subject and determine whether (i) to reject the request and communicate this to the data subject; (ii) an extension of time is reasonably required to perform the request, and if so to communicate this to the data subject; or (iii) to move to the next step.
4.	Take the requested action or compile and provide the requested information.	The requested action is to be performed in the time limits laid down by law or, where an extended time period is required as permitted by law and communicated to the data subject, within the extended period.
5.	Record the rights request and the actions taken.	A record of all rights requests is to be kept to ensure the exercise of data subject rights has been facilitated. Also, to demonstrate compliance with the law, especially where the rights request has been rejected.

4. Facilitation of Data Subject Rights

The rights of data subjects in the UK or EU shall be facilitated in line with the following:

Right to be informed

Data subjects shall be informed about the processing of their personal data using privacy notices, in the manner set out in the Sister Data Protection Policy.

Right of access

A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which Sister holds about them. Sister will normally be required to respond to SARs within one month of receipt. This can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension. The decision to inform the data subject that there is a need for an extension to the period for responding or to charge reasonable fees shall only be made by the Sister Data Protection Officer.

Sister does not charge a fee for the handling of normal SARs. We reserve the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Right to rectification

If a data subject informs Sister that personal data held by Sister is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification,

within one month of receipt the data subject's notice. This can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension. The decision to inform the data subject that there is a need for an extension to the period rectification shall only be made by the Sister Data Protection Officer
In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

The right to erasure (also referred to as the 'right to be forgotten')

Data subjects may request that Sister erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for Sister to hold that personal data with respect to the purpose for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to Sister holding and processing their personal data;
- The data subject objects to Sister holding and processing their personal data (and there is no overriding legitimate interest to allow Sister to continue doing so);
- The personal data has been processed unlawfully; or
- The personal data needs to be erased in order for Sister to comply with a particular legal obligation.

Unless Sister has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. This can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension. The decision to inform the data subject that there is a need for an extension to the period required to erase the personal data shall only be made by the Sister Data Protection Officer.

In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so)

The right to restrict processing

Data subjects may request that Sister ceases processing the personal data it holds about them. If a data subject makes such a request, Sister shall retain only the amount of personal data pertaining to that data subject that it is necessary to ensure that no further processing of their personal data takes place.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

The right to data portability

Where data subjects have given their consent to Sister to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between Sister and the data subject, data subjects have the right to receive a copy of their personal data in a structured, commonly used and machine-readable format and to transmit it to other data controllers (e.g. other organisations).

In exercising this right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

All requests for copies of personal data for the purposes of data portability shall be complied with within one month of the data subject's request. This can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension. The decision to inform the data subject that there is a need for an extension to the period required to provide copies of the personal data shall only be made by the Sister Data Protection Officer.

The right to object

Data subjects have the right to object to Sister processing their personal data based on legitimate interests (including profiling) and direct marketing (including profiling).

Where a data subject objects to Sister processing their personal data based on its legitimate interests, Sister shall cease such processing forthwith, unless it can be demonstrated that Sister legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

Where a data subject objects to Sister processing their personal data for direct marketing purposes, Sister shall cease such processing forthwith.

Rights with respect to automated decision-making and profiling

In the event that Sister uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions, to request human intervention, to express their own point of view and to obtain an explanation of the decision from Sister.

The right described in immediately above does not apply in the following circumstances:

- The decision is necessary for the entry into, or performance of, a contract between Sister and the data subject;
- The decision is authorised by law; or
- The data subject has given their explicit consent.

Schedule 1
Data Subject Rights Request Form Template
This form can be amended as appropriate with the authorisation of the Data Protection Officer.

Sister

Data Subject Rights Request Form

About this Form
This form is used by Sister to confirm the identity of the data subject (of a third party acting on behalf of the data subject) making a rights request and the nature of the rights to be exercised.
Once completed, please send the form and any attachments to dpolondon@sister.net or Sister, 17-18 Hayward's Place, London, EC1R 0EQ, marked for the attention of the Data Protection Officer.

Data Subject's Details

Please confirm your contact details:

Title	
First Name	
Surname	
Address	
Telephone No.	
Email Address	

Identity Verification

Please provide us with further information to enable us to verify your identity. If you provide additional documents for this purpose, please only send copies to us and not originals:

Details of further information to enable us to verify your identity	

Third Parties Acting for the Data Subject

If you are acting on behalf of a data subject, please confirm the nature of your relationship with the data subject and provide us with proof that you are entitled to act on behalf of the data subject. If you provide additional documents for this purpose, please only send copies to us and not originals Please also provide us with your contact details:

Details of your relationship with the data subject and proof provided	
Your Title	
Your Surname	
Your Address	
Your Telephone No.	
Your Email Address	

Nature of Request

Please confirm the type of request you are making and provide us with any further information to help us facilitate your request:

Type of Request	☐ Subject access right request	☐ Right to Rectification request	☐ Right to erasure request	☐ Right to restrict processing request
	☐ Right of portability request	☐ Right to object request	☐ Automated decision making request	☐ Withdrawal of consent
Additional information related to your request				

Declaration

I confirm I am the data subject named above:

Signature	
Full Name	
Date	

OR

I confirm I am the third party named above and that I am entitled to act on behalf of the data subject named above:

Signature	
Full Name	
Date	

BYOD (Bring Your Own Device)

Sister have opted to offer their employees the option to use their own devices for company use subject to management approval and appropriate controls.

Employees who prefer to use their personally-owned IT equipment for work purposes must be explicitly authorised to do so, must secure corporate data to the same extent as on corporate IT equipment, and must not introduce unacceptable risks (such as malware) onto these devices or the corporate networks by failing to secure their own equipment.

A BYOD is deemed to be any equipment (e.g. Mobile, PDA, Tablet, Laptop, etc.) used by Sister staff (or their contractors) to store or process Sister data that is not directly owned by or the responsibility of Sister.

In contrast to the information and communications technology devices owned by the organisation, personally owned devices (PODs) are devices owned by employees or by third parties (such as suppliers, consultancies and maintenance contractors). Authorised employees and third parties may wish to use their PODs for work purposes, for example making and receiving work phone calls and text messages on their own personal cell phones, using their own tablet computers to access, read and respond to work emails, or working in a home-office.

Bring Your Own Device (BYOD) is associated with a number of information security risks such as:

- Loss, disclosure or corruption of corporate data stored on the personal device.
- Loss or theft of the device, or external storage used on the device.
- Incidents involving threats to, or compromise of, the personal device and hence the corporate infrastructure and other information assets (e.g. malware infection or hacking).
- Potential to breach compliance with applicable laws, regulations and obligations such as data protection and privacy legislation.
- Accidental or deliberate breaches of intellectual property rights for group information created, stored, processed or communicated on these personal devices in the course of work for Sister.

Due to management's concerns about information security risks associated with staff using these personal devices, individuals who wish to opt-in to BYOD must be authorised by their line manager and must explicitly accept the requirements laid out in this standard.

Management reserves the right not to authorise individuals, or to withdraw the authorisation, if they deem personal devices not to be appropriate and in the best interests of the group.

The business directors and the owners and users of personally owned devices share responsibilities for the security of information stored or processed by the BYOD device.

Nothing in this standard affects Sister's ownership of corporate information, including all work-related intellectual property created in the course of work on personal devices.

Persons accepting this standard must be aware that:

- While employees have a reasonable expectation of privacy over their personal information on their own equipment, Sister's right to control its data and manage personal devices may expose such personal information.
- To reduce the possibility of such disclosure staff should keep their personal data separate from the business data in such a way as to logically separate directories and ensure private and personal data is clearly named and separated (e.g. "Private data" and "Sister data").
- They should take care not to infringe other people's privacy rights.

All relevant employees are responsible for complying with this standard and other Sister policies and standards at all times, ensuring such software and operating systems / environments on the POD are up to date and patched.

Data Retention Policy

1. Introduction

1.1 This Policy sets out the obligations of Sister Pictures Limited, a company registered in England and Wales under number 09631264 whose registered office is at 17-18 Hayward's Place, London, EC1R 0EQ (the "Company") regarding retention of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

1.2 The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.3 The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life or sexual orientation.

1.4 Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

1.5 In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

- where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
- when the data subject withdraws their consent;
- when the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;
- when the personal data is processed unlawfully (i.e. in breach of the GDPR);
- when the personal data has to be erased to comply with a legal obligation; or
- where the personal data is processed for the provision of information society services to a child.

1.6 This Policy sets out the type(s) of personal data held by the Company for insert specific purposes, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of. For further information on other aspects of data protection and compliance with the GDPR, please refer to the Company's Data Protection Policy.

2. Aims and Objectives

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR.

2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

3.1 This Policy applies to all personal data held by the Company of AND/OR by third-party data processors processing personal data on the Company's behalf.

3.2 Personal data is stored in the following ways and in the following locations:

- computers permanently located in the Company's premises at its registered office, any other Company offices and at any production office relating to a production;
- laptop computers and other mobile devices provided by the Company to its employees;
- computers and mobile devices owned by employees, agents, and sub-contractors used in accordance with the Company's Bring Your Own Device ("BYOD") Policy;
- physical records stored at its registered office, any other Company office and at any production office relating to a production;

4. Data subject rights and data integrity

4.1 All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

4.2 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used as set out in Part 12 of the Company's Data Protection Policy, and how long the Company will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.3 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy) and the right to restrict the Company's use of their personal data as set out in the Company's Data Protection Policy.

5. Technical and Organisational Data Security Measures

5.1 The following technical measures are in place within the Company to protect the security of personal data. Please refer to the Company's Data Protection Policy for further details.

- All emails containing personal data must be marked "confidential".
- Personal data may only be transmitted over secure networks.
- Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative.
- Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient.
- All personal data transferred physically should be transferred in a suitable container marked "confidential".
- No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from Sister Senior Management Team or Data Protection Officer.
- All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely.
- Personal data must be handled with care at all times and should not be left unattended or on view.
- Computers used to view personal data must always be locked before being left unattended.
- All electronic copies of personal data should be stored securely using passwords.
- All passwords used to protect personal data should be changed if we believe they have become compromised and should be secure.
- Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method.
- All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available.
- No software may be installed on any Company-owned computer without approval.
- Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Sister Data Protection Officer or, in relation to a programme, the producer of any programme to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

5.2 The following organisational measures are in place within the Company to protect the security of personal data. Please refer to the Company's Data Protection Policy for further details.

- All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy.
- Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company.
- All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so.
- All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised.

- All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times.
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.
- The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.
- All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy.
- All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy.
- Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure unless otherwise agreed by Sister Business Affairs.

6. Data Disposal

6.1 On the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

- personal data stored electronically (including any and all backups thereof) shall be deleted securely;
- special category personal data stored electronically (including any and all backups thereof) shall be deleted securely;
- personal data stored in hardcopy form shall be shredded**;** and
- special category personal data stored in hardcopy form shall be shredded.

7. Data Retention

7.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

- The type of personal data in question;
- The objectives and requirements of the Company;
- The purpose(s) for which the data in question is collected, held, and processed;
- The Company's legal basis for collecting, holding, and processing that data;
- The category or categories of data subject to whom the data relates;

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

7.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Type of data	**Purpose of data**	**Review period**	**Retention period or criteria**	**Comments**
Accident Books, accident records/reports	Compliance with a legal obligation	Annual	3 years from the date of last entry (or if the accident involves a child/young adult, then	**Statutory authority:** The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995

			until that person reaches the age of 25).	(RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances
Accounting records	Compliance with a legal obligation	Annual	7 years	**Statutory authority:** Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006.
Income tax and NI returns, income tax records and correspondence with HMRC	Compliance with a legal obligation	Annual	7 years after the end of the financial year to which they relate	**Statutory authority:** The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631).
Medical records under the Health Protection (Coronavirus) Regulations 2020	Compliance with a legal obligation	Annual	1 year	**Statutory authority**: The Health Protection Regulations 2020 (2020/129)
Medical records and details of biological tests under the Control of lead at Work Regulations	Compliance with a legal obligation	Annual	40 years from the date of the last entry	**Statutory authority:** The Control of Lead at Work Regulations 1998 (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676).
Medical records under the control of Asbestos at Work Regulations: medical records containing details of employees exposed to asbestos and medical examination certificates	Compliance with a legal obligation	Annual	Medical records: 40 years from the date of the last entry Medical examination certificates: 4 years from the date of issue	**Statutory authority:** The Control of Asbestos at Work Regulations 2002 (SI 2002/ 2675). Also see the Control of Asbestos Regulations 2006 (SI 2006/2739) and the Control of Asbestos Regulations 2012 (SI 2012/632)
Medical records as specified by the Control of Substances Hazardous to Health (COSHH)	Compliance with a legal obligation	Annual	40 years from the date of last entry	**Statutory authority:** The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).
Medical records under the ionising radiations regulations 1999	Compliance with a legal obligation	Annual	Until the person reaches 75 years of age but in any event for at least 50 years	**Statutory authority**: The Ionising Radiations Regulations 1999 (SI 1999/3232).
Records of tests and examinations of control systems	Compliance with a legal obligation	Annual	5 years from the date on which the tests were carried out	**Statutory authority:** The Control of Substances Hazardous

and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)				to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).
Records relating to children and young adults	Compliance with a legal obligation	Annual	Until the child/young adult reaches the age of 21	**Statutory authority:** Limitation Act 1980.
Retirement benefits schemes – records of notifiable events, for example relating to incapacity	Compliance with a legal obligation	Annual	6 years from the end of the scheme year in which the event took place	**Statutory authority:** The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	Compliance with a legal obligation and necessary for the performance of the employment contract	Annual	3 years after the end of the tax year in which the maternity period ends	**Statutory authority:** The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended.
Wage/salary records (also overtime, bonuses, expenses)	Compliance with a legal obligation and necessary for the performance of the employment contract	Annual	6 years	**Statutory authority:** Taxes Management Act 1970
National minimum wage records	Compliance with a legal obligation	Annual	3 years after the end of the pay reference period following the one that the records cover	**Statutory authority:** National Minimum Wage Act 1998
Records relating to working time	Compliance with a legal obligation	Annual	2 years from date on which they were made	**Statutory authority:** The Working Time Regulations 1998 (SI 1998/1833)
Application forms and interview notes (for unsuccessful candidates)	Compliance with a legal obligation and processing personal data in the pursuit of the Company's legitimate interest	Annual	3 years	
Parental leave	Necessary for the performance of the employment contract	Annual	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance	
Pension scheme investment policies	Necessary for the performance of the employment contract	Annual	12 years from the ending of any benefit payable under the policy	
Personnel files and training records (including disciplinary records and working time records) for employees and freelancers	Necessary for the performance of the employment/freelance contract and compliance with a legal obligation	Annual	6 years after engagement ceases	
Redundancy details, calculations of	Processing personal data in the pursuit of	Annual	6 years from the date of redundancy	

payment, refunds, notification to the Secretary of State	the Company's legitimate interest			
Statutory sick pay records, calculations, certificates, self-certificates	Processing personal data in the pursuit of the Company's legitimate interest	Annual	6 years after the employment ceases	
Time cards	Necessary for the performance of the employment contract	Annual	2 years after audit	
Trade union agreements	Processing personal data in the pursuit of the Company's legitimate interest	Annual	10 years after ceasing to be effective	

8. Roles and Responsibilities

8.1 The Company's Data Protection Officer is Laura Crowley, Commercial Director.

8.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

8.3 The Data Protection Officer shall be directly responsible for ensuring compliance with the above data retention periods throughout the Company**.**

8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

Personal Data Breach Procedure

Introduction

This personal data breach procedure (this "procedure") sets out the procedure to be followed by all Sister employees, workers and contractors ("personnel/you/your") in the event of a personal data breach affecting data subjects in the UK or EU (a "data breach"). This procedure must be read together with the Sister Data Protection Policy.

This is a Sister procedure and applies to all personnel. It has been prepared with due regard to the Data Protection Act 2018 and to local data protection laws in the countries in which we operate.

A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. The Data Protection Act 2018 requires:

- any data breach likely to result in a risk to the rights and freedoms of data subjects in the UK or EU to be reported to the appropriate data protection authority without undue delay and, where feasible, within 72 hours of becoming aware of it; and
- any data breach likely to result in a high risk (that is, a higher risk than that described immediately above) to the rights and freedoms of data subjects in the UK or EU to be reported to the affected data subjects without undue delay except where specific conditions are met.

You must follow this procedure when responding a data breach. Any failure to do so may result in disciplinary action.
For ease of reference, the data breach notification obligations are summarised in the flow chart at Schedule 1.

Steps to Follow

In the event of a data breach, the following steps must be followed:

No.	Step	Action
1.	A potential data breach is identified.	All potential data breaches must be reported urgently to the Sister Data Protection Officer by email to dpolondon@sister.net setting out the details of the data breach.
2.	Investigate whether a data breach has occurred.	Sister shall immediately undertake an initial investigation to establish whether a breach has occurred.
3.	Assess the risks to affected data subjects.	The initial investigation shall include an assessment of the risks to rights and freedoms of data subjects affected by the data breach.
4.	Notify the appropriate data protection authority where required.	If it is determined that the breach is likely to result in a risk to data subjects in the UK or EU, the appropriate data protection authority shall be notified without undue delay in the manner set out at part 4 of this procedure.
5.	Notify affected data subjects where required.	If it is determined that the breach is likely to result in a high risk to data subjects in the UK or EU the affected data subjects shall be notified without undue delay in the manner set out at part 5 of this procedure.
6.	Record the data breach and details of the actions taken.	A record of all data breaches must be kept, using the Sister Personal Data Breach Register (held by the Sister Data Protection Officer) to demonstrate accountability and compliance with the law.

Initial Investigation

Upon first being informed of, or upon first identifying, a potential data breach, Sister shall immediately undertake a short period of initial investigation. The investigation shall be led by the team supported by such other persons as shall be deemed necessary. The Sister Data Protection Officer shall be kept informed as to the progress and findings of the investigation at all times and shall advise on the steps to be taken to ensure compliance with our legal obligations.

The investigation shall establish with a reasonable degree of certainty whether a data breach has taken place and whether the breach is likely to result in:

- No risk to rights and freedoms of data subjects;
- Risk to rights and freedoms of data subjects; or
- High risk to the rights and freedoms of the data subjects.

Risk exists where the data breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Factors to be considered when assessing the risk to data subjects shall include:

- The type of breach
- The nature, sensitivity and volume of personal data
- Ease of identification of individuals
- Severity of consequences for individuals
- Any special characteristics of the individual
- The number of affected individuals

A data breach involving 'sensitive personal data' shall always be considered likely to result in a risk to data subjects and potentially a high risk, depending on the factors listed above.

'Sensitive personal data' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person; data concerning health or data concerning a natural person's sex life or sexual orientation; and data relating to criminal convictions and offences.

The decisions reached in the initial investigation must be documented and signed-off by the Sister Data Protection Officer and include one of the following conclusions:

a) The data breach does not require notification because there are no risks to rights and freedoms of data subjects in the UK or EU;

b) The data breach requires notification to the appropriate data protection authority only, because there are risks to rights and freedoms of data subjects in the UK or EU; or

c) The data breach requires notification both to the appropriate data protection authority and to the affected data subjects because the risks to rights and freedoms of data subjects in the UK or EU are high (except where measures have subsequently been taken to mitigate the high risk to data subjects, in which case notification to data subjects is not required).

Notifying the Data Protection Authority

Where the data breach is likely to result in a risk to the rights and freedoms of affected data subjects in the UK or EU, Sister shall report the personal data breach to the appropriate data protection authority without undue delay, and where feasible not later than 72 hours after having become aware of the personal data breach.

The appropriate data protection authority shall be the national data protection authority in the country in which the breach took place, or, in the case of a cross-border breach involving personal data of data subjects in the UK or EU, Information Commissioner's Office (ICO).

Where a data breach notification to the appropriate data protection authority is not made within 72 hours, it shall be accompanied by the reasons for the delay.

At the time of notification, Sister shall provide the following information to the appropriate data protection authority:

a) A description of the nature of the breach;

b) The categories of personal data affected;

c) Approximate number of data subjects affected;

d) Approximate number of personal data records affected;

e) Name and contact details of the Sister Data Protection Officer;

f) Details of the likely consequences of the breach;

g) Any measures that have been or will be taken to address the breach, including mitigation; and

h) Additional information relating to the data breach (additional information may be provided in phases after the 72 hour time limit provided reasons for the delay are provided)

Notifying Affected Data Subjects

Subsection A: Obligation to notify

Where the data breach is likely to result in a high risk to the rights and freedoms of affected data subjects in the UK or EU, Sister shall report the data breach to the affected data subjects without undue delay, except where Subsection B of this part applies.

The notification to the data subject shall describe in clear and plain language the nature of the breach and must cover:

a) Name and contact details of the Sister Data Protection Officer where one has been designated, or other point of contact from whom more information may be obtained;

b) A description of the likely consequences of the personal data breach; and

c) A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects.

The notification shall also offer advice to the data subject regarding actions they may be able to take to reduce the risks associated with the personal data breach, where appropriate (e.g. advising that passwords should be reset where access credentials have been compromised).

The notification should be communicated to the affected data subjects directly using a dedicated message, preferably email. Public communication may be used where communicating directly with every affected data subject would involve a disproportionate effort. Suitable public communications include prominent website banners or notifications and advertisements in print media.

Subsection B: When notification is not required

The obligation to notify data subjects in the UK or EU affected by a data breach set out in Subsection A of this part shall not apply where:

a) Sister has implemented measures to the personal data affected by the data breach which render the personal data unintelligible to any person who is not authorised to access it (such as state-of-the-art encryption); or

b) Sister has taken steps following the breach to ensure that the high risk to the rights and freedoms of data subjects referred to in Subsection A of this part is no longer likely to materialise (such as immediately identifying and taking action against an individual who has accessed personal data before they were unable to do anything with it).

Recording the Data Breach

All data breaches shall be recorded in the Sister Personal Data Breach Register, regardless of whether or not the breach needs to be notified to a data protection authority or to data subjects.

Schedule 1
Summary of Data Breach Notification Obligations