SOCIETY DATA PROTECTION POLICY
&
PRIVACY NOTICE

Policy Number: 36

Document Control

Owner	Reviewers	Approver
Head of People & Performance	Head of People & Performance Head of Internal Audit SMT	Head of People & Performance Head of Internal Audit Head of I&C

Version	Date Issued	Status	Description	Review Date
Finalv1.0	8th May 2018	Final	New policy for GDPR.	Apr 2019

Policy

This document sets out the Society's policy on the protection of information relating to employees, workers, contractors, volunteers and interns (referred to as employees). Protecting the confidentiality and integrity of personal data is a critical responsibility that the Society takes seriously at all times. The Society will ensure that data is always processed in accordance with the provisions of relevant data protection legislation, including the General Data Protection Regulation (GDPR).

Key Definitions

- **"Data processing"** Data processing is any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.
- "**Personal data"** Personal data is any information identifying a data subject (a living person to whom the data relates). It includes information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers the Society possesses or can reasonably access. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
- **"Sensitive personal data"** Sensitive personal data is a special category of information which relates to a data subject's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. It also includes personal data relating to criminal offences and convictions.

Privacy Notice

This policy, together with the information contained in the table of employees data appended to the policy, constitutes a privacy notice setting out the information the Society holds about employees, the purpose for which this data is held and the lawful basis on which it is held. The Society may process personal information without employees' knowledge or consent, in compliance with this policy, where this is required or permitted by law.

If the purpose for processing any piece of data about employees should change, the Society will update the table of employees data with the new purpose and the lawful basis for processing the data and will notify employees.

Fair Processing of Data

Fair processing principles

In processing employees' data the following principles will be adhered to. Personal data will be:

- Used lawfully, fairly and in a transparent way;
- Collected only for valid purposes that are clearly explained and not used in any way that is incompatible with those purposes (see appendix);
- Relevant to specific purposes and limited only to those purposes;
- Accurate and kept up to date;
- Kept only as long as necessary for the specified purposes; and
- Kept securely with controlled access limited to those who need for this purpose.

Lawful processing of personal data

Personal information will only be processed when there is a lawful basis for doing so. Most commonly, the Society will use personal information in the following circumstances:

- when it is needed to perform employees' contracts of employment;
- when it is needed to comply with a legal obligation; or
- when it is necessary for the Society's legitimate interests (or those of a third party) and employees' interests and fundamental rights do not override those interests.

The Society may also use personal information in the following situations, which are likely to be rare:

- when it is necessary to protect employees' interests (or someone else's interests); or
- when it is necessary in the public interest [or for official purposes].

Lawful processing of sensitive personal data

The Society may process special categories of personal information in the following circumstances:

- In limited circumstances, with explicit written consent;
- in order to meet legal obligations;
- when it is needed in the public interest, such as for equal opportunities monitoring [or in relation to the Society's occupational pension scheme]; or
- when it is needed to assess working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, the Society may process this type of information where it is needed in relation to legal claims or where it is needed to protect an employees interests (or someone else's interests) and the employee is not capable of giving consent, or where an employee has already made the information public. The Society may use particularly sensitive personal information in the following ways:

- information relating to leave of absence, which may include sickness absence or family related leave, may be used to comply with employment and other laws;
- information about employees' physical or mental health, or disability status, may be used to ensure health and safety in the workplace and to assess fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits;
- information about race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, may be used to ensure meaningful equal opportunity monitoring and reporting; and
- information about trade union membership may be used to pay trade union premiums, register the status of protected employees and to comply with employment law obligations.

Lawful processing of information about criminal convictions

The Society envisages that it will hold information about criminal convictions. The Society will only use this information where it has a legal basis for processing the information. This will usually be where such processing is necessary to carry out the Society's obligations. Less commonly, the Society may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect an employees interests (or someone else's interests) and the employee is not capable of giving consent, or where the employee has already made the information public.

Where appropriate, the Society will collect information about criminal convictions as part of the recruitment process or may require employees to disclose information about criminal convictions during the course of employment.

Consent to data processing

The Society does not require consent from employees to process most types of employee data. In addition, the Society will not usually need consent to use special categories of personal information in order to carry out legal obligations or exercise specific rights in the field of employment law. If an employee fails to provide certain information when requested, the Society may not be able to perform the contract entered into with the employee (such as paying the employee or providing a benefit). The Society may also be prevented from complying with legal obligations (such as to ensure the health and safety of employees).

In limited circumstances, for example, if a medical report is sought for the purposes of managing sickness absence, employees may be asked for written consent to process sensitive data. In those circumstances, employees will be provided with full details of the information that sought and the reason it is needed, so that employees can carefully consider whether to consent. It is not a condition of employees' contracts that employees agree to any request for consent.

Where employees have provided consent to the collection, processing and transfer of personal information for a specific purpose, they have the right to withdraw consent for that specific processing at any time. Once the Society has received notification of withdrawal of consent it will no longer process information for the purpose or purposes originally agreed to, unless it has another legitimate basis for doing so in law.

Automated decision making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention.

The Society does not envisage that any decisions will be taken about employees using automated means, however employees will be notified if this position changes.

Collection & Retention of Data

Collection of data

The Society will collect personal information about employees through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. The Society may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

The table of employees data appended to this policy relates to information which is collected at the outset of employment. From time to time, the Society may collect additional personal information in the course of job-related activities throughout the period of employment. If the Society requires to obtain additional personal information, this policy will be updated or employees will receive a separate privacy notice setting out the purpose and lawful basis for processing the data.

Retention of data

The Society will only retain employees' personal information for as long as necessary to fulfil the purposes it was collected for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of personal information are set out in the table of employees data appended to this policy.

When determining the appropriate retention period for personal data, the Society will consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for which the personal data is processed, whether the Society can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances the Society may anonymise personal information so that it can no longer be associated with individual employees, in which case the Society may use such information without further notice to employees. After the data retention period has expired, the Society will securely destroy employees' personal information.

Data Security & Sharing

Data security

The Society has put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Access to personal information is limited to those employees, agents, contractors and other third parties who have a business need to know. e.g. The Society's pension provider. They will only process personal information on the Society's instructions and are subject to a duty of confidentiality. The Society expects employees handling personal data to take steps to safeguard personal data of employees (or any other individual) in line with this policy.

Data sharing

The Society requires third parties to respect the security of employees data and to treat it in accordance with the law. The Society may share personal information with third parties, for example in the context of the possible sale or restructuring of the business. The Society may also need to share personal information with a regulator or to otherwise comply with the law.

The Society may also share employees data with third-party service providers where it is necessary to administer the working relationship with employees or where the Society has a legitimate interest in doing so. The following activities are carried out by third-party service providers: pension administration, benefits provision and administration.

Employees Rights & Obligations

Accuracy of data

The Society will conduct regular reviews of the information held by it to ensure the relevancy of the information it holds. Employees are under a duty to inform the Society of any changes to their current circumstances. Where an Employee has concerns regarding the accuracy of personal data held by the Society, the Employee should contact a member of the People and Performance team to request an amendment to the data.

Employees rights

Under certain circumstances, employees have the right to:

- **Request access** to personal information (commonly known as a "data subject access request").
- **Request erasure** of personal information.
- **Object to processing** of personal information where the Society is relying on a legitimate interest (or those of a third party) to lawfully process it.
- **Request the restriction of processing** of personal information.
- **Request the transfer** of personal information to another party.

If an employee wishes to make a request on any of the above grounds, they should contact the Data Privacy Manager in writing. Please note that, depending on the nature of the request, the Society may have good grounds for refusing to comply. If that is the case, the employee will be given an explanation by the Society.

Data subject access requests

Employees will not normally have to pay a fee to access personal information (or to exercise any of the other rights). However, the Society may charge a reasonable fee if the request for access is clearly unfounded or excessive. Alternatively, the Society may refuse to comply with the request in such circumstances.

The Society may need to request specific information from employees to help confirm their identity and ensure the right to access the information (or to exercise any of the other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Compliance with this Policy

The Society's responsibility for compliance

The Data Privacy Manager is tasked with overseeing compliance with this policy. If employees have any questions about this policy or how the Society handles personal information, they should contact the Data Privacy Manager. Employees have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Data security breaches

The Society has put in place procedures to deal with any data security breach and will notify employees and any applicable regulator of a suspected breach where legally required to do so.

In certain circumstances, the Society will be required to notify regulators of a data security breach within 72 hours of the breach. Therefore, if an employee becomes aware of a data security breach it is imperative that they report it to the Data Privacy Manager (Head of People and Performance) immediately.

Privacy by design

The Society will have regard to the principles of this policy and relevant legislation when designing or implementing new systems or processes (known as "privacy by design").

Independent Guidance

Comprehensive independent guidance and information is available on the Information Commissioners website at https://ico.org.uk/

EMPLOYEES DATA						
Type of personal data	**Sensitive data?**	**Purpose of processing**	**Potential transfer to third parties**	**Lawful basis for processing**	**Grounds for processing sensitive personal data**	**Retention period**
Contact details	No	Administering the employment contract	HMRC / Professional advisors	Legal obligation	N/A	6 years post-employment
Date of birth	No	Equal opportunities monitoring	Professional advisors	Legal obligation	N/A	6 years post-employment
Gender	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation	employment purposes	6 years post-employment
Marital status	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation	employment purposes	6 years post-employment
Information about race	Yes	Equal opportunities monitoring	Professional advisors	Legal Obligation	employment purposes	6 years post-employment
Information about ethnicity	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation	employment purposes	6 years post-employment
Information about religious beliefs	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation	employment purposes	6 years post-employment
Next of kin / emergency contact	No	Safety and security	N/A	Legal obligation	N/A	During employment
NI number	No	Payroll	HMRC / Professional advisors	Legal obligation	N/A	6 years post-employment
Salary information	No	Payroll	HMRC / Professional advisors	Legal obligation	N/A	6 years post-employment
Bank details	No	Payroll	HMRC	Legal obligation	N/A	6 months post-employment
Tax details	No	Payroll	HMRC	Legal obligation	N/A	6 years post-employment
Pension details	No	Payroll / liaising with pension providers	HMRC / pension providers	Legal obligation	employment purposes	75 years post-employment
Benefits information	No	Providing benefits to employees	Benefit providers / Professional advisors	Legal obligation	N/A	6 years post-employment
Driving license	No	Making recruitment decisions / ascertaining ability to work	N/A	Legal obligation	N/A	6 years post-employment
CV	No	Making recruitment decisions / ascertaining ability to work	N/A	Legal obligation	N/A	6 years post-employment
Right to work documents	Yes	Checking right to work in the UK	Professional advisors	Legal obligation	employment purposes	2 years post-employment
Sick leave details	No	Managing absence	Professional advisors	Legal obligation	employment purposes	6 years post-employment
Performance details	No	Managing performance	Professional advisors	Legal obligation	N/A	6 years post-employment
Qualifications	No	Making recruitment decisions / ascertaining ability to work	Professional advisors	Legal obligation	N/A	6 years post-employment

Employment history	No	Making recruitment decisions / ascertaining ability to work	N/A	Legal obligation	N/A	6 years post-employment
Information about disability	Yes	Managing staff / health and safety requirements / ascertaining fitness to work	Professional advisors	Legal obligation	employment purposes	6 years post-employment
Training records	No	Education, training and development requirements	Professional advisors	Legal obligation	N/A	6 years post-employment
Professional memberships	No	Education, training and development requirements	N/A	Legal obligation	N/A	6 years post-employment
Disciplinary and grievance information	No	Staff management	Professional advisors	Legal obligation	N/A	6 years post-employment
CCTV footage	No	Safety and security	Professional advisors	Legitimate interests	N/A	6 years post-employment
Swipe card records	No	Managing timekeeping and absence / safety and security	Professional advisors	Legal obligation	N/A	6 years post-employment
Information about use of IT systems	No	Ensuring network and data security / staff management	Professional advisors	Legitimate interests	N/A	6 years post-employment
Photographs	No	Safety and security	N/A	Legitimate interests	N/A	During employment
Trade union membership	Yes	Deducting trade union fees	Professional advisors	Legal obligation	employment purposes	6 years post-employment
Health records	Yes	Managing absence / ascertaining fitness to work	Professional advisors	Legal obligation	employment purposes	6 years post-employment
Criminal convictions and offences	Yes	Making decisions about recruitment / continued employment	Professional advisors	Legal obligation	employment purposes	6 years post-employment