

LONDON MATHEMATICAL SOCIETY

DATA PROTECTION POLICY

CONTENTS

Introduction	1
Registration with the Information Commissioner’s Office	2
Scope of the Policy	2
Data Protection Officer	2
Responsibilities Under the Six Principles of the GDPR / DPA.....	3
Processing Data	4
Legal Bases for Processing Personal Data.....	4
Additional Conditions to Process Special Category Personal Data	5
Individuals’ Rights under GDPR / DPA.....	5
Individuals’ Rights under GDPR / DPA and Different Legal Bases	6
Privacy Statements and Privacy Notice	6
Data Register	6
Collection of Personal Data	7
Retention & Disposal of Personal Data	7
Data Sharing	7
Data Security and Data Breach Procedures	8
Data Transfer outside the United Kingdom (UK)	9
LMS EU GDPR Representative	9
Responsibilities Of Individual Data Users	9
Summary Of The Society’s Data Protection Policy	11
Annex I: Legal Bases.....	13
Annex II : Additional Condition Of Processing for SpecialCategory of Data:	14

INTRODUCTION

1. Under the UK General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018, organisations, including the Society, which process “personal data” have a legal obligation to abide by the regulations set out under the Act to protect that personal data.
 - i. Personal Data is defined as information relating to a person who can be identified either directly or indirectly in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person; and includes information about that person e.g. name, address, bank details, CCTV images, IP addresses, biometric data
 - ii. Special Categories of Personal Data is defined as information relating to the person’s race/ethnic origin; political opinion; religious or philosophical beliefs; trade union membership; physical or mental health condition; sexual life; genetic and biometric data used to uniquely identify that person.

POLICY



2. In particular, the Society must:
 - i. Have a legal basis to process personal data and, in the case of processing special category personal data, an additional condition to process those data;
 - ii. only collect personal information that is needed for a specific purpose;
 - iii. keep the personal data secure;
 - iv. not disclose data to unauthorised third parties
 - v. ensure the data is accurate and up to date;
 - vi. only hold as much personal data as is required, and only for as long as it is required for a specific purpose;
 - vii. respect individuals' rights under the GDPR/DPA;
 - viii. pay a data protection fee to the Information Commissioners Office (ICO)
 - ix. report severe breaches to the ICO within 72 hours of becoming aware of the breach.

REGISTRATION WITH THE INFORMATION COMMISSIONER'S OFFICE

3. The Society is registered with the Information Commissioner's Office (ICO) as a fee-paying Data Controller, which means the Society determines the purposes and manner in which personal data is to be processed, and it pays a fee to the ICO.
 - i. The ICO maintains a public register of all fee-paying Data Controllers including the name and address.
 - ii. The Society's registration number is Z6256165 and may be reviewed at <https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/>

SCOPE OF THE POLICY

4. This policy covers all personal data held and processed by the London Mathematical Society.
 - i. This includes all data processed using, and held on, electronic equipment and/or in a structured paper filing system.
 - ii. The policy covers all Society staff and others acting on behalf of the Society, e.g. Council and Committee members, or who otherwise have access to the Society's data including external data processors e.g. auditors, publishers.

DATA PROTECTION OFFICER

5. The Society's Data Protection Officer is the Executive Secretary. All queries about the Society's Data Protection Policy and all requests for access to personal data should be addressed to the Data Protection Officer.

RESPONSIBILITIES UNDER THE SIX PRINCIPLES OF THE GDPR/DPA

6. As the Data Controller, the Society is responsible for, and should be able to demonstrate, compliance with the 6 principles of the GDPR/DPA 2018.

Principle	What it Says	What it Means
Principle a	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals;	To process personal data lawfully, there should be a valid legal basis and, in the case of special category data, an additional condition should be met. To process personal data fairly, the Society should consider the rights of and impact on individuals. To process personal data in a transparent manner, individuals should be provided with information on how their data will be used by the Society via the Privacy Notice.
Principle b	Personal data shall 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	Data collected for one purpose should not be used for another without fresh consent. For instance, an email list of event participants should not be used for direct email marketing unless the participants have consented to receive these emails.
Principle c	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.	Only the information required to do the job should be collected and used.
Principle d	Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.	Data quality should be maintained to ensure that it is: Accurate – any inaccuracies should be corrected as soon as possible; individuals have the right to have their data rectified. If the inaccurate data is no longer needed, then it should be deleted. Up to Date – any personal data processed should be the most up to date version and older versions should be deleted/destroyed.
Principle e	Personal data shall be 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.	When personal data are no longer required, they should be destroyed/deleted securely, in line with Society's data retention schedule.

Principle f	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	Personal data must be kept secure by: Secure storage - Paper files should be locked away and electronic records should be protected by passwords and encryption, where appropriate. Shared responsibly – personal data should only be shared with the individual’s consent or where the individual would reasonably expect their data to be shared e.g. members subscribing to the European Mathematical Society would expect us to share their contact details with the EMS so they can receive their Newsletter.
-------------	---	--

PROCESSING DATA

7. In relation to information or data, *processing* means obtaining, recording or holding data, including:
 - i. organisation, adaptation or alteration of the information or data
 - ii. retrieval, consultation or use of the information or data
 - iii. disclosure of the information or data by transmission, dissemination or otherwise making available, or
 - iv. alignment, combination, blocking, erasure or destruction of the information or data.
8. The Society must use one of six legal bases to process any personal data and the Society must use one of six legal bases and an additional condition to process *special category* personal data provided.

LEGAL BASES FOR PROCESSING PERSONAL DATA

9. To process personal data lawfully, the Society should have a valid legal basis so at least one of the following six legal bases must be used to process personal data. NB All legal bases are equal and they are not listed in order of priority or preference:
 - i. Consent - With the Consent of the Data Subject
For example, the Society would rely on consent to send direct marketing material by email to individuals.
 - ii. Contract - To perform duties to fulfil a contractual obligation
For example, the Society would rely on contract to provide membership services to fulfil its contract with LMS Members.
 - iii. Legal Obligation - To meet a meet a legal obligation
For example, the Society would rely on legal obligation to disclose information to HMRC for tax and gift aid purposes.
 - iv. Legitimate Interests - To fulfil a legitimate interest of the LMS (on the understanding that it does not override the interests of the data subject)

For example, the Society would rely on legitimate interests to facilitate communication with and between LMS Committee members so they can carry out their duties.
 - v. Vital Interests - To protect the vital interests of data subjects.

POLICY



For example, the Society would rely on vital interests to disclose information to paramedics in the event that someone needs emergency medical treatment and is physically incapable of giving consent to share the information.

- vi. Public Task - To process personal data in the exercise of official authority or to perform a specific task in the public interest that is set out in law

The Society does not rely on this legal basis because the Society is not a public authority nor does it exercise official authority or carry out tasks in the public interest.

10. These legal bases are recorded in the Society's audit register against each purpose for processing personal data and are referred to in the Society's Privacy Notice. Where the purpose for processing personal data changes, the Society will review whether the new purpose is compatible with the original purpose so that it can continue to use the same legal basis. Annex I lists these legal bases in full.

ADDITIONAL CONDITIONS TO PROCESS SPECIAL CATEGORY PERSONAL DATA

11. To process special category personal data lawfully, the Society should have a valid legal basis as outlined above and an additional condition should also be met e.g. explicit consent from the individual. Annex II lists these additional conditions in full.

INDIVIDUALS' RIGHTS UNDER GDPR/DPA

12. The Society recognises individuals have the following rights under GDPR/DPA:

- i. The Right to be informed about how the Society collect and process their personal data, including its purposes. The Society informs individuals of its data processing and its purposes via Privacy Statements at the time of collection, which link to the Privacy Notice. If the Society has collected individuals' data from another source, the Society will provide them with the Privacy Notice as soon as possible.
- ii. The Right of Access of individuals to their personal data so that they are aware of and can verify the lawfulness of its processing of their personal data.
- iii. The Right to Rectification of their personal data. While the Society tries to keep its data as accurate as possible, the Society will rectify inaccurate personal data, or complete it if it is incomplete.
- iv. The Right to Erasure (also known as 'the right to be forgotten'). Individuals have the right to have personal data erased, in particular circumstances.
- v. The Right to Restrict Processing their personal data. When processing is restricted, the Society is permitted to store individuals' personal data, but not use it.
- vi. The Right to Data Portability – that is, individuals have the right to obtain and reuse their personal data, which they have provided to the Society, for their own purposes across different services. It allows them to move, copy or transfer their personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- vii. The Right to Object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.
- viii. The right to withdraw consent (if applicable). Where the Society relies on their consent to process their personal data, they have the right to withdraw their consent at any time.

13. Further information on how to deal with individuals' requests under these rights are detailed in the

Individuals Rights' Procedures.

INDIVIDUALS' RIGHTS UNDER GDPR/DPA AND DIFFERENT LEGAL BASES

14. The Society recognises that the lawful basis for its processing can also affect which rights are available to individuals. For example, some rights will not apply as detailed below:

	Right to Erasure	Right to Portability	Right to Object
Consent			No – <i>but right to withdraw consent</i>
Contract			No
Legal Obligation	No	No	No
Vital Interests		No	No
Public Tasks	No	No	
Legitimate Interests		No	

Source: (Information Commissioner's Office (ICO), 2018)

PRIVACY STATEMENTS AND PRIVACY NOTICE

15. The Society uses layered approach to informing individuals about how it will process their data by providing Privacy Statements at the time of data collection, which refer to the Society's main Privacy Notice (available on the LMS website; <https://www.lms.ac.uk/privacy-notice>).
16. To ensure fair and lawful processing, it is the Society's policy to provide, or make readily available, a 'Privacy Statement' when collecting personal data either directly or indirectly, which will include the following information:
- i. the identity of the Society,
 - ii. the source of the personal data
 - iii. the purposes for processing the data and the legal basis (and additional condition, if applicable)
 - iv. whether the data will be shared and if so, with whom
 - v. that the data will be held in compliance with the Society's data retention schedule and then destroyed/deleted securely
 - vi. that the individual has particular rights under the GDPR in relation to the legal basis for processing
 - vii. reference to the Society's Privacy Notice.

DATA REGISTER

17. The Society keeps a register of the personal data it processes, which includes information on:
- i. WHY ... is personal data processed?
The business function and the purpose for processing.
 - ii. WHOSE ... personal data is processed?
The categories of individuals affected by processing.

- iii. WHAT ... personal data is processed?
The categories of personal data used in processing, the legal bases used for processing, including details of legitimate interests and, if applicable, the special conditions used for processing personal data.
 - iv. WHEN ... is personal data processed?
When the personal data is obtained, to whom, it may be disclosed and why and how long it is retained for.
 - v. WHERE ... is personal data processed?
Where processing occurs and how the data is kept secured
18. The data register lists the personal data by business functions which are specified as the department processing the personal data. Each purpose for processing has been assigned to a specific staff member within that department and who will be responsible for the data that they process. Staff will work with the Data Protection Officer by:
- i. updating the Data Protection Officer on any new purposes for processing personal data, especially if this will require notifying the ICO.
 - ii. making available any personal data required to comply with a Subject Access Request.
 - iii. ensuring the data is kept secure and access is restricted only to authorised personnel.
19. The register is reviewed annually to ensure that any changes to processing personal data is recorded.

COLLECTION OF PERSONAL DATA

20. To ensure that data collected is relevant to the Society's purposes and not excessive for any specified purpose, the Society regularly reviews what data is collected and the purposes for which it is collected. Where the Society plans to make big changes to the way it processes personal data, it will undertake a Data Protection Impact Assessment before it begins to process personal data.

RETENTION & DISPOSAL OF PERSONAL DATA

21. To ensure that data is not held for longer than necessary, the Society abides by the *Data Retention Schedule* which outlines how long data may be kept, which data is suitable for archiving and which data can be disposed of or deleted.
22. To ensure safe disposal, all physical copies of personal data must be placed in the confidential waste bin for secure disposal or shredded onsite. Digital copies, including emails, must be permanently deleted when they are no longer needed. Personal data held on portable devices such as laptops and USB sticks must be regularly cleaned so that personal data is not stored for longer than is necessary.

DATA SHARING

23. The Society will not disclose data to third parties, except where it is legally obliged to do so, where it is necessary to carry out its functions or where it is in the vital interest of the individual. Where the Society discloses data to third parties to process data on behalf of the Society (otherwise known as Data Processors), data processing agreement clauses will be included in any contracts where the Data Processor processes personal data on behalf of the Society.
24. Where practicable and unless it is exempt from doing so, the Society will seek consent from/inform individuals before disclosing data to third parties e.g. informing journal subscribers that their contact details will be passed on to the publishers who will send journals to them.

25. Examples of where the Society is exempt from seeking consent from the individual include:
- i. the prevention or detection of crime
 - ii. the apprehension or prosecution of offenders
 - iii. the assessment or collection of tax or duty
 - iv. other exemptions under the GDPR/DPA.
26. Before disclosing data to third parties, the *Data Sharing Checklist* must be read and checked
27. If Officers, Members of the Society's Council and Committee Chairs wish to access the LMS database to contact members for purposes in the interest of the Society only, the request must be made using the *Data Sharing Request Form* and sent to the Data Protection Officer, who will assess the request for sharing data and respond with a *Data Sharing Decision Form*.
28. Personal data must not be disclosed to an unauthorised third party either verbally or in writing. If in doubt, consult the Data Protection Officer.

DATA SECURITY AND DATA BREACH PROCEDURES

29. The Society will take appropriate technical, physical and organisational measures to prevent the unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data.
30. Personal data must be kept securely and measures to prevent unauthorised access to personal data include:
31. Technical measures
- i. Restricted access to PCs and laptops via individual passwords.
 - ii. Restricted access to SharePoint and Office 365 via passwords and two-factor authentication.
 - iii. Limited USB stick access to the server
 - iv. Limited use of portable devices to process and store personal data.
 - v. Computers are password-protected. Laptop, USB stick or any other portable electronic media are password-protected.
 - vi. Access to the LMS online database restricted to certain LMS staff.
 - vii. Access to the LMS online database is password-protected.
32. Physical measures
- i. Paper records are locked in a filing cabinet, drawer or room.
 - ii. Locked filing cabinets with keys held only by authorised personnel.
 - iii. Restricted access for non-members of staff to offices.
33. Organisational measures
- i. *Work from Home* procedures, which should be followed to ensure that personal data is kept secure when it is processed off-site.
 - ii. *Personal Data considered by Council/Committee* document circulated at the first meeting of Council/Committee after every AGM so new and continuing Council/Committee members are notified of their responsibilities with respect to handling personal data on behalf of the Society.

- iii. Regular staff training
34. These measures are examples and the list is not exhaustive.
35. The Society will make every reasonable effort to ensure that data is not disclosed accidentally. In the event of a data breach, this must be reported to the Data Protection Officer and the steps in the *Data Security Breach Procedure* must be followed. These steps include assessing the severity of the breach. Severe breaches must be reported to the ICO within 72 hours of becoming aware of the breach.

DATA TRANSFER OUTSIDE THE UNITED KINGDOM (UK)

36. The Society may, on occasion, transfer personal data to organisations in countries or territories outside the United Kingdom. In these cases, the Society will ensure the organisation receiving the personal data has provided adequate safeguards by using standard data protection clauses and/or contractual clauses authorised by the ICO in contracts with these organisations.
37. Transfers may normally be made with the individual's informed consent; or where it is necessary for the performance of a contract between the individual and the Society or for pre-contractual steps taken at the individual's request; or where it is necessary for the performance of a contract made in the interests of the individual between the Society and a third party.
38. The Society may, on occasion, seek references and reviews on funding proposals, journal articles and Prize nominations from individuals based outside the United Kingdom. As these transfers are infrequent, the GDPR provides that personal data may still be transferred outside the UK. Such transfers are permitted only where the transfer is not repetitive (similar transfers are not made on a regular basis); involves data related to only a limited number of individuals; is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and is made subject to suitable safeguards put in place by the Society (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.
39. In these cases, the Society is obliged to inform the ICO of the transfer and provide additional information to individuals via Privacy Statements and the Privacy Notice, except in the case of Prize nominations which remain confidential. For example, prospective Research School organisers will be advised that their proposal will be sent to referees, who could be based outside the UK, for peer-review.

LMS EU GDPR REPRESENTATIVE

40. As the Society offers goods and services to individuals who are based in the European Economic Area (EEA) but it does not have an office, branch or other establishment based within the EEA, the Society recognises that it is required by the EU GDPR to have an EU GDPR Representative. To comply, the Society has authorised an EU GDPR Representative, in writing, to act on its behalf regarding the Society's compliance with the EU GDPR and to deal with supervisory authorities and data subjects in respect of the Society's compliance with the EU GDPR. The Society has ensured that the LMS EU GDPR Representative is based in an EEA state where some of the data subjects, whose personal data are processed by the Society, are based. The Society has advised individuals and supervisory authorities of the LMS EU GDPR Representative in the Privacy Notice on its website. Any changes to the LMS EU GDPR Representative will be communicated via the online Privacy Notice and in other correspondence, as appropriate.

RESPONSIBILITIES OF INDIVIDUAL DATA USERS

41. All members of the Society and all staff who record and/or process personal data in any form are

POLICY



responsible for ensuring that personal data which is held by the Society, or on behalf of the Society:

- i. is processed lawfully and fairly
- ii. is processed only for specified purposes
- iii. is relevant and not excessive
- iv. is accurate and kept up to date
- v. is not kept for longer than necessary for the specified purpose
- vi. is disposed of securely, when no longer required
- vii. is processed in accordance with the rights of the individual
- viii. is made available promptly when requested by the Data Protection Officer to respond to a Subject Access Request
- ix. is kept securely
- x. is not disclosed either verbally or in writing or otherwise to any unauthorised third party, and that every reasonable effort will be made to see that data is not disclosed accidentally.
- xi. is not transferred outside the UK unless the Data Protection Officer is satisfied there is an adequate level of protection.

42. It is the policy of the Society to ensure that all members of the Society and its staff are aware of data protection legislation and their individual responsibilities in this connection through one or more of the following:

- i. the Data Protection Policy
- ii. Procedures relating to Data Protection
- iii. Training

Updated policy approved by Council
2 July 2021

Approved by Council
19 October 2018

Revised by Council
29 June 2018

Original policy approved by Council
29 June 2012

SUMMARY OF THE SOCIETY'S DATA PROTECTION POLICY

1. The Society's Data Protection Policy demonstrates how the Society will comply with its legal obligations under the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018 and the Privacy and Electronic Communications Regulations 2003. In summary, through appropriate management and strict application of criteria and controls, the Society will:
2. When collecting data (either directly from individuals or indirectly from other sources):
 - i. Provide or, have readily available, a Privacy Statement which outlines specified purposes for which the data is collected;
 - ii. Seek consent from the individual to process and hold personal data, where Consent is specified as the legal basis for processing;
3. Process personal data using at least one of the six legal bases under Article 6 of the GDPR/ Part 1 of Schedule 2 of the DPA 2018.
4. Process special categories of personal data when using at least one of the six legal bases under Article 6 of the GDPR/ Part 1 of Schedule 2 of the DPA 2018 AND at least one of the special conditions under Article 6 of the GDPR/ Parts 1 and 2 of Schedule 1 of the DPA 2018.
5. Respect and support the rights of individual individuals as outlined in Articles 12-23 of the GDPR/Part 2 of Schedule 20 of the DPA 2018, including the individual's right to:
 - i. The Right to be informed about how the Society collect and process their personal data, including its purposes.
 - ii. The Right of Access of individuals to their personal data.
 - iii. The Right to Rectification of their personal data.
 - iv. The Right to Erasure (also known as 'the right to be forgotten').
 - v. The Right to Restrict Processing their personal data.
 - vi. The Right to Data Portability obtain and reuse their personal data, which individuals have provided to the Society, for their own purposes across different services.
 - vii. The Right to Object to processing of their personal data.
 - viii. The Right to withdraw consent (if applicable).
6. Inform individuals about how it will process their personal data through Privacy Statements and the Privacy Notice.
7. Maintain a data register of how it collects and processes data, including the specified purposes for processing.
8. Collect and process data that is relevant and sufficient to meet the requirements of those specified purposes or to comply with any legal obligations
9. Ensure data is accurate and kept up to date
10. Retain data only for a period of time that is considered reasonable for the Society to fulfil its specified purposes and/or legal obligations and dispose of data securely when it is no longer required.
11. Carefully consider any requests to share personal data and not disclose personal data to un-authorised third parties
12. Put in place, and regularly review, Data Sharing Agreements with any Data Processors who are contracted to process personal data on behalf of the Society
13. Protect personal information through putting in place and maintaining suitable technical, physical and organisational security measures and report severe breaches to the ICO within 72 hours of being aware of the breach.
14. Not transfer personal information outside the UK without being satisfied that an adequate level of protection is guaranteed.

POLICY



15. Ensure that all members of the Society and its staff are aware of data protection legislation and their individual responsibilities in this connection through providing adequate staff training.

ANNEX I: LEGAL BASES

CONSENT

1. Where consent is used as the legal basis for processing personal data, the Society will seek a positive opt-in consent from individuals for the Society to process and hold their personal data, especially when collecting special category personal data, when using the personal data to send direct marketing emails and/or the use or sharing of the data may be objectionable or unexpected by the individual.
2. The Society will make requests for consent clear, concise and granular so that the Society collects separate consent for separate purposes. Any third parties who rely on consent will be named in the request. Individuals will be asked to consent via a positive opt-in action e.g. ticking a box or sending an email. Consent will be recorded so that the Society can demonstrate who, when, how, and what the Society told individuals.
3. Further information on how to collect and record consent are detailed in the *Collecting and Using Consent Procedures*.

LEGITIMATE INTERESTS

4. Where the Legitimate Interests is used as the legal basis for processing personal data, the Society will inform individuals via its Privacy Statements and Privacy Notice that their data is processed under this legal basis. It will use individuals' data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. The Society recognises that it is taking on extra responsibility for considering and protecting people's rights and interests.
5. The Society will use and keep a record of Legitimate Interest Assessments in which it will identify a legitimate interest; show that the processing is necessary to achieve it; and balance it against the individual's interests, rights and freedoms. Individuals will have opportunity to object to any processing of their personal data which will be considered by the Society. However, the Society will reserve the right to process personal data if it can demonstrate that the processing does not override the individuals' interests, rights and freedoms.
6. Further information on how to identify, demonstrate and record legitimate interests are detailed in the *Using Legitimate Interests Procedures*.

CONTRACT

7. Where consent is used as the legal basis for processing personal data, the Society can rely on this lawful basis if it needs to process someone's personal data:
 - i. to fulfil its contractual obligations to them; or
 - ii. because they have asked the Society to do something before entering into a contract (e.g. provide a quote).
8. It does not apply if the Society needs to process one person's details but the contract is with someone else.
9. It does not apply if the Society takes pre-contractual steps on its own initiative or at the request of a third party.
10. Note that, in this context, a contract does not have to be a formal signed document, or even written down, as long as there is an agreement which meets the requirements of contract law. Broadly speaking, this means that the terms have been offered and accepted, both parties intend them to be

POLICY



legally binding, and there is an element of exchange (usually an exchange of goods or services for money, but this can be anything of value). However, this is not a full explanation of contract law, and if in doubt, seek legal advice.

LEGAL OBLIGATION

11. Where Legal Obligation is used as the legal basis for processing personal data, the Society can rely on this lawful basis if it needs to process the personal data to comply with a common law or statutory obligation. This does not apply to contractual obligations. The processing must be necessary. The Society should be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out its obligation.

VITAL INTERESTS

12. Where Vital Interests are used as the legal basis for processing personal data, the Society can rely on vital interests as its lawful basis if it needs to process the personal data to protect someone's life. The processing must be necessary. If the Society can reasonably protect the person's Vital Interests in another less intrusive way, this basis will not apply. The Society cannot rely on Vital Interests as a legal basis for processing in the cases of health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.

ANNEX II: ADDITIONAL CONDITION OF PROCESSING FOR SPECIAL CATEGORY OF DATA:

1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. processing relates to personal data which are manifestly made public by the data subject;
6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;
10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.