Data Protection Policy

The Honourable Society of Lincoln's Inn

Introduction

The Honourable Society of Lincoln's Inn (Lincoln's Inn) regards the lawful and correct processing of personal and sensitive data as an integral part of its purpose. Lincoln's Inn believes this is vital for maintaining the confidence of members, volunteers, employees and other stakeholders about whom we process data, and ourselves.

Policy Statement

This Data Protection Policy explains how Lincoln's Inn will meet its legal obligations concerning confidentiality and data security standards. The requirements within the policy are primarily based upon the UK GDPR and Data Protection Act (DPA) 2018, which is the key piece of legislation covering data security and confidentiality of personal and sensitive personal data.

- Lincoln's Inn will fully implement all aspects of the UK GDPR and Data Protection Act 2018.
- Lincoln's Inn will ensure all employees and others handling personal data are aware of their obligations and rights under the UK GDPR and Data Protection Act 2018.
- Lincoln's Inn will implement adequate and appropriate physical and technical measures and organisational measures to ensure the security of all data contained in or handled by its systems.

The main focus of this policy is to provide guidance about the protection, sharing and disclosure of personal data, but it is important to stress that maintaining confidentiality and adhering to data protection legislation applies to anyone handling personal data or personal sensitive data on behalf of Lincoln's Inn.

Registration with the Information Commissioner

The DPA requires every data controller (i.e. organisation) to register with the Information Commissioner's Office (ICO) and outline the categories of data they hold about people, and what they do with it.

Lincoln's Inn is registered with the ICO to 'process personal information to enable us to provide a service for members as specified in our constitution; administer records in relation to property management, training & education; to promote the interests of the organisation; manage our employees and volunteers and maintain our own accounts and records. Our processing also includes the use of CCTV systems for the prevention of crime.'

Definitions of Personal Data and Sensitive Personal Data

- All identifiable member data
- All identifiable employee data
- All identifiable volunteer data
- All identifiable resident and tenant data
- All other personal data processed by Lincoln's Inn

Examples of personal identifiable data Lincoln's Inn processes include:

- Names, addresses, emails, phone numbers and other contact information
- Membership numbers
- Beneficiary financial information
- National insurance numbers and payroll data
- Photographs, video and audio recordings

Certain types of data are regarded as sensitive and attract additional legal protection. Sensitive personal data is considered to be any data that could identify a person such as:

- The racial or ethnic origin of the individual
- Political opinions or affiliations
- Religious beliefs or other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence
- Any proceeding for any offence committed or alleged to have been committed or disposal of such proceedings or the sentence of court in such proceedings
- Bank account details, any official identification details such as passport or driving licence numbers etc.

Data Protection Principles

The seven Data Protection principles that lie at the heart of the DPA give the Act its strength and purpose. To this end, Lincoln's Inn fully endorses and abides by the principles of data protection. Specifically, the seven principles require that:

- **Principle 1:** Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met. See the document 'Guidance for: Collecting and Processing Data Correctly'.
- **Principle 2:** Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- **Principle 3:** Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.
- **Principle 4:** Personal data shall be accurate and kept up to date as far as is possible.
- **Principle 5:** Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

- **Principle 6:** Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.
- **Principle 7:** Appropriate measures and records shall be in place to be able to demonstrate compliance against the other principles.

Personal data and sensitive personal data must not be used other than for the specific purpose required to deliver a product or service. The individual should always know that their data is being processed. When that data is especially sensitive, consent is required before the data can be processed by Lincoln's Inn.

All data collected from people under the age of 16 (unless there are concerns about mental capacity in which case this should be extended) is to be treated as sensitive personal data.

A record can be in computerised and/or in a physical format. It may include such documentation as:

- Manually stored paper files e.g. membership records, employee records
- Hand written notes
- Letters to and from Lincoln's Inn
- Electronic records
- Printouts
- Photographs
- Videos and tape recordings

Backup data (i.e. archived data or disaster recovery records) also falls under the DPA; however, a search within them should only be conducted if specifically asked for by an individual as an official Subject Access Request.

Rights of Access by Individuals

The DPA gives every living person (or their authorised representative) the right to apply for access to the personal data which organisations hold about them irrespective of when and how they were compiled, i.e. hand written records, electronic and manual records held in a structured file. This is called a Subject Access Request. The DPA treats personnel data relating to employees, members and clients alike.

Practical Implications

Understanding and complying with the seven Data Protection Principles is the key to understanding and complying with the Inn's responsibilities as the data controller. Therefore, Lincoln's Inn will, through appropriate management, and strict application of criteria and controls:

- Ensure that there are lawful grounds for using the personal data
- Ensure that the use of the data is fair and meets one of the specified conditions

- Only use sensitive personal data where we have obtained the individual's explicit consent (unless an exemption applies)
- Only use sensitive personal data, if it is absolutely necessary
- Explain to individuals, at the time their personal data is collected, how that information will be used
- Only obtain and use personal data for those purposes which are known to the individual
- Ensure personal data is only used for the purpose it was given. If we need to use the data for other purposes, further consent will be obtained.
- Only keep personal data that is relevant to Lincoln's Inn
- Keep personal data accurate and up to date
- Only keep personal data for as long as is necessary
- Always adhere to our Subject Access Request Procedure and be receptive to any queries, requests or complaints made by individuals in connection with their personal data
- Always allow individuals to opt out of receiving mass communications, with the exception of core administrative emails
- Always offer an option to 'opt in' when consent is needed to share personal data unless there is a statutory or legal reason to do so
- Take appropriate technical and organisational security measures to safeguard personal data.

In addition, Lincoln's Inn will ensure that:

- There is an employee appointed as the Security Information Risk Owner with specific responsibility for Data Protection in Lincoln's Inn. This is currently the Assistant Under Treasurer.
- Everyone managing and handling personal data and sensitive personal data has undertaken annual training, understands that they are legally responsible for following good data protection practice and has read and signed the Inn's Data Protection Policy.
- Everyone managing and handling personal data and sensitive personal data is appropriately supervised by their line manager.
- Enquiries about handling personal data and sensitive personal data are dealt with promptly.
- Methods of handling personal data and sensitive personal data are clearly described in polices and guidance.
- A review and audit of data protection arrangements is undertaken annually. This will take place each year in June of the year in question.
- Methods of handling personal data and sensitive personal data are regularly assessed and evaluated by the Security Information Risk Owner and relevant members of the Executive team.
- Performance with personal data and sensitive personal data handling is regularly assessed and evaluated by the Security Information Risk Owner and relevant members of the Executive team.

- Formal written Data Processing Agreements are in place before any personal data and sensitive personal data is transferred to a third party.

Roles and Responsibilities

Maintaining confidentiality and adhering to data protection legislation applies to everyone at Lincoln's Inn. Lincoln's Inn will take necessary steps to ensure that everyone managing and processing personal data understands that they are responsible for following good data protection practice. Employees will receive training and sign the Inn's Data Protection Policy as part of their induction. Volunteers such as Student Representatives and temporary staff will also be asked to sign the policy and will undertake an online training course.

All employees, volunteers and contractors have a responsibility to:

- Observe all guidance and codes of conduct in relation to obtaining, using and disclosing personal data and sensitive personal data
- Obtain and process personal data and sensitive personal data only for specified purposes
- Only access personal data and sensitive personal data that is specifically required to carry out their activity or work
- Record data correctly in both manual and electronic records
- Ensure any personal data and sensitive personal data is held is kept secure
- Ensure that personal data and sensitive personal data is not disclosed in any form to any unauthorised third party
- Ensure personal data and sensitive personal data is sent securely
- Read and sign the policy, directing any questions to the Assistant Under Treasurer.

Failure to adhere to any guidance in this policy could mean an individual(s) being criminally liable for deliberate unlawful disclosure under the DPA. This may result in criminal prosecution and/or disciplinary action.

All Managers are responsible for:

- Determining if their operational area holds personal data and sensitive personal data and ensuring that the data is adequately secure, access is controlled and that the data is only used for the intended purposes
- Providing clear messaging to their teams about data protection requirements and measures
- Ensuring personal and sensitive personal data is only held for the purpose intended
- Ensuring personal and sensitive personal data is not communicated or shared for non-authorised purposes
- Ensuring personal and sensitive personal data is password protected when transmitted or appropriate security measures are taken to protect when in transit or storage.

Security Information Risk Owner – The Assistant Under Treasurer holds the post of Security Information Risk Owner. Responsibilities include:

- Ensuring compliance with legislation principles
- Ensuring notification of processing of personal data and sensitive personal data to the ICO is up to date
- Providing guidance and advice to employees in relation to compliance with legislative requirements
- Auditing data protection arrangements annually
- Reporting on any breaches of Data Protection legislation
- Ensuring those handling personal data are aware of their obligations by producing relevant policies, auditing the arrangements and ensuring the relevant people receive training

In the Security Information Risk Owner's absence, advice can be gained from http://www.ico.gov.uk.

Responsibility of the Under Treasurer – As the Senior Executive, the Under Treasurer has overall responsibility for Data Protection within Lincoln's Inn. Lincoln's Inn has a duty to ensure that the requirements of the DPA are upheld.

The Information Commissioner's Office (ICO) – The Information Commissioner's Office is responsible for overseeing compliance e.g. investigating complaints, issuing codes of practice and guidance, maintaining a register of Data Protection Officers. Any failure to comply with DPA may lead to investigation by the ICO which could result in serious financial or other consequences for Lincoln's Inn.

Breach of Policy

In the event that an employee fails to comply with this policy, the matter may be considered as misconduct and dealt with in accordance with Lincoln's Inn's Disciplinary Policy.

Any individuals or organisations with whom Lincoln's Inn data has been shared may be personally liable for any breach of the DPA.

Dealing with a Data Breach

If a data breach is suspected, the person who identified the breach should immediately:

- Notify the Assistant Under Treasurer (AUT)
- Complete and return the Data Incident Reporting Form, which is available from the Security Information Risk Owner.

Following notification of a breach, the Security Information Risk Owner will take the following action as a matter of urgency:

- Implement a recovery plan, which will include damage limitation
- Assess the risks associated with the breach

- Inform the appropriate people and organisations that the breach has occurred
- Review the Inn's response and update our information security

Policies and Procedures

This policy should be read in conjunction with the following policies and guidance documents:

- Bring Your Own Device Policy
- Data Protection Operational Policy – Handling Data
- Data Protection Policy - Master
- Data Protection Policy for Employees
- IT Security Policy
- Records Management Policy
- Guidance for Collecting and Processing Data Correctly
- Guidance for Dealing with a Data Subject Access Request
- Guidance for Identity Verification
- Guidance for Password Protecting a Document
- Guidance for Posting Records Containing Personal Data
- Guidance for Travelling Safely with Data
- Managing email
- Lincoln's Inn Data Processing Agreement
- Data Incident Reporting Form

Glossary of Terms

Data Subject
An individual who is the subject of personal data or sensitive personal data. This includes employees, members, volunteers, clients, residents and tenants.

Data Controller
A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data and sensitive personal data are, or are to be processed.

The data controller is Lincoln's Inn.

Data Processor
In relation to personal data or sensitive personal data, this refers to any person who processes that data on behalf of the data controller but is not employed by them.

Data Processors include but are not limited to mailing houses to which Lincoln's Inn sends mailing lists and external companies who have access to Lincoln's Inn's data.

Third Party

In relation to personal data or sensitive personal data, this refers to any person other than the data subject, the data controller, or any data processor or other person authorised to process data for data controller or processor. For example, the Police or HMRC.

Processing
Recording or holding data or carrying out any operations on that data including organising, altering or adapting it; disclosing the data or aligning, combining, blocking or erasing it.

Data Extractor
The person who takes data from a data source, such as a database, which may then be used for further activity. For example, an employee querying the database to print a list of address labels for letters.

Data Breach
A failure leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or sensitive personal data.

Subject Access Request
A written, signed request (which includes emails and other written formats) from an individual to see data which Lincoln's Inn holds about them. The Data Controller must provide all such information in a readable form within one month of receipt of the request, or once the identity has been verified.