**Policy Owner:** The Information Security Governance Committee.

# Overview:

Set out below is LSL Property Services plc’s (**LSL**) Data Protection policy (**Policy**), which applies to the LSL group of companies (**LSL Group**).

Each Division of the LSL Group will appoint a Data Protection Officer (**DPO**) who is responsible for the compliance of their Division with this Policy.

The Divisional DPO’s contact details can be found in the Appendix to this Policy.

Each member of the LSL Group will in addition appoint an individual Data Protection Steward (**DPS**) who is responsible for assisting the Divisional DPO with the compliance of their subsidiary trading companies/business areas to this Policy. Each of the DPSs will be assisted by individuals who are charged to assist them in the discharge of their responsibilities at an operational level.

The Group Data Protection Steward is the General Counsel and Company Secretary (**Group DPS**).

# Introduction and Status:

* 1. This Policy sets out the legal requirements and internal LSL rules in relation to the Processing of Personal Data by LSL and LSL Group companies.
  2. This Policy forms part of the LSL Group’s Information Security Framework, which has been approved by the LSL Board.
  3. This Policy does not form part of any employee's employment contract and it may be amended at any time. Please note that any breach of this Policy will be taken seriously and may result in disciplinary action.
  4. The collection, use and disclosure of Personal Data in relation to employees is also the subject of a separate HR Data Protection Policy that is maintained by the LSL Group’s Human Resources function and is available on People Matters or the relevant Divisional intranet site.
  5. This Policy uses a number of terms which are capitalised. The meaning of those terms is set out below in section 4 (**Definitions**) of this Policy.
  6. The collection and use of Personal Data by businesses in the UK must comply with UK data protection laws.

These laws are primarily contained in the GDPR and Data Protection Act 2018 (**DPA**) together with guidance issued by the IC (see details of the Data Sharing Code of Practice below).

* 1. This Policy is drafted for use by LSL Group companies, which all operate in the UK. It sets out the conditions under which LSL Group companies will process Personal Data relating to employees, customers, suppliers and other third parties.

* 1. This Policy will support LSL Group companies in ensuring compliance with the GDPR and DPA. Failure to comply can, in certain cases, lead to criminal sanctions (with directors and other company officers potentially facing personal liability) and liability for damages, in addition to negative publicity/reputational damage and fines (the IC can fine an organisation up to 20 000 000 EUR, or up to 4% of its group’s total annual turnover in the preceding financial year, whichever is higher - see also section [20](#_bookmark9) below which details some of the powers of the IC and the ICO).

# LSL Group's Legal Requirements:

* 1. Everyone has rights with regard to how their Personal Data is handled. During the course of their activities LSL Group companies will collect, store and process Personal Data and LSL Group companies recognise the need to treat it in an appropriate and lawful manner.
  2. LSL Group companies may process Personal Data about the following types of individuals:
     1. current, past and prospective employees (including temporary members of staff);
     2. current, past and prospective suppliers and service providers;
     3. current, past and prospective customers; and
     4. other individuals that we communicate with or about.
  3. Everyone’s Personal Data is subject to legal safeguards set out in applicable data protection laws including the GDPR, DPA and the Privacy and Electronic Communications Regulations 2003 (**PECR**). The GDPR, DPA and PECR impose restrictions on how LSL Group companies process Personal Data.
  4. The GDPR, DPA and PECR are enforced by the IC and the ICO also issues good practice recommendations and guidance which LSL Group companies must have regard to in addition to the strict legal requirements.

# Responsibility for data protection:

* 1. All employees are responsible for ensuring compliance with applicable data protection laws and with this Policy.

Any questions or concerns about the operation of this Policy should be referred to the Group DPS.

* 1. The Divisional DPOs are responsible for data protection within their subsidiary trading companies/business areas, although for the avoidance of doubt the Divisional DPOs are not personally liable for the data protection compliance of their subsidiary trading companies/business areas. Set out below is a summary of the key responsibilities of the DPOs who will be assisted by the LSL Group companies/business areas DPS:

1. to inform and advise the LSL Group and LSL Group employees about their obligations to comply with the GDPR and other data protection laws;
2. to monitor compliance with the GDPR, other data protection laws and this Policy;
3. to manage internal data protection activities, raise awareness of data protection issues, train employees and conduct internal audits;
4. to advise on, and to monitor, data protection impact assessments; and
5. to cooperate with the ICO and be the first point of contact for the ICO and for individuals whose data is being processed by the LSL Group.
   1. Details of the Divisional DPOs are set out in the Appendix to the Policy and details of the DPS are available from the relevant DPO.
   2. Information Security Officers (**ISO**) exist across LSL’s Divisions and the ISO’s are responsible for creating and instituting measures designed to protect the information held on the LSL Group’s systems. The ISO’s are available to provide support and assistance to Divisional DPOs and the DPS community and unless alternative arrangements apply, can be contacted via the business units IT helpdesk support function.
   3. If you consider that this Policy has not been followed in respect of Personal Data about yourself or others you should raise the matter with either your line manager, the Divisional DPO or the DPS for your company/business area. You can also raise any concerns via the Group Whistleblowing process (see the Combined Ethics Policy for details of how you can report a breach). Copies of all LSL Group policies are available on People Matters or from relevant Divisional intranet sites.

# Definitions:

* 1. This section of the Policy includes definitions of the most relevant data protection terms. The definitions are based on the definitions contained in Article 4 of the GDPR, and include additional plain English explanations of the various terms.
  2. **Code** means the Data Sharing Code of Practice issued by the ICO and dated May 2011 or any replacement to it.
  3. **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.
  4. **Data Subjects** for the purpose of this policy include all living individuals about whom LSL Group companies hold Personal Data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their Personal Data.
  5. **Data Controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any Personal Data is processed. They have a responsibility to comply with the GDPR and establish practices and policies in line with the GDPR. Each LSL Group company that processes Personal Data is likely to be the Data Controller of Personal Data used in that business. There are also circumstances where LSL Group companies may also act as Data Processors on behalf of other LSL Group companies or third parties outside the LSL Group.
  6. **Data Users** include employees whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following the LSL Group’s data protection and security policies at all times.
  7. **Data Processors** include any person who processes Personal Data on behalf of a Data Controller. Employees of Data Controllers are excluded from this definition but it could include suppliers or agents which handle Personal Data on behalf of a Data Controller and LSL Group companies who process Personal Data on behalf of other LSL Group companies.
  8. **GDPR** means the General Data Protection Regulation (EU) 2016/679.
  9. **IC and ICO** refer to the Information Commissioner and the Information Commissioners Office, which is the organisation responsible for the GDPR, DPA and PECR (see sections 1 and 18 for further details or visit www.ico.gov.uk).
  10. **Personal Data** means data relating to a living individual who can be identified from that data (or from that data and other information which is in the possession of, or is likely to come into the possession of the Data Controller) 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 living individual. Personal Data can be factual (such as a name, address or date of birth, bank details etc.) or it can be an opinion (such as a performance appraisal). Personal Data includes information held electronically (such as information stored on computers, laptops, memory sticks, tablets, smart phones and on LSL Group companies’ IT systems), as well as information held in structured hardcopy filing systems. Personal Data may also be held in audio and media files such as telephone recordings, video and CCTV recordings and photographs. Personal Data also includes any expression of opinion about an individual and any indication of the intentions of a person in respect of the individual.
  11. **Processing** is any activity that involves use of Personal Data. It includes obtaining, recording or holding Personal Data, or carrying out any operation or set of operations on Personal Data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties or otherwise making Personal Data available.
  12. **Special Category Personal Data** includes information about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning physical or mental health or condition or a person’s sex life or sexual orientation.
  13. **Sharing** is defined in the Code as the disclosure of Personal Data from one or more organisation(s) to a third party organisation(s), or the sharing of data between different parts of an organisation. Further details and examples of data sharing are set out in section 18 below.
  14. **Subject Access Request** is a request made by an individual to an organisation seeking details of the Personal Data held about them and processed by the organisation. Any individual can ask any organisation to provide them with full details of the Personal Data held about them (subject to certain conditions). A Subject Access Request must be made in writing (including by email) and the relevant information must be provided by the relevant LSL Group company promptly and in any event within one month of receipt of the request (see section [14](#_bookmark7) below for further information on dealing with Subject Access Requests).

# GDPR Principles:

* 1. This section includes a description of the seven data protection principles set out in Article 5 of the GDPR, together with a more detailed explanation of the meaning of some of those principles.
  2. The GDPR and DPA govern the Processing of Personal Data.
  3. The GDPR differentiates between Personal Data, Special Category Personal Data and Personal Data relating to criminal convictions and offences. The GDPR affords greater protection to Special Category Personal Data and Personal Data relating to criminal convictions and offences.
  4. The GDPR obliges LSL and LSL Group companies to Process Personal Data (including Special Category Personal Data and Personal Data relating to criminal convictions and offences) in accordance with the seven core principles which are called the "Data Protection Principles". The requirements of these principles are summarised in sectio[n 5.5](#_bookmark0) below:
  5. The seven data protection principles require that:

1. Personal Data must be processed fairly and lawfully and in a transparent manner;
2. Personal Data must be obtained only for one or more specified, explicit and legitimate purposes, and should not be processed in any manner incompatible with that purpose or those purposes;
3. Personal Data must be adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed;
4. Personal Data must be accurate and where necessary kept up to date;
5. Personal Data must not be kept longer than necessary for the purpose or purposes for which the Personal Data was obtained by LSL Group companies;
6. Personal Data must be kept secure using appropriate technical and organisational security measures to protect against the unauthorised or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data; and
7. A Data Controller shall be responsible for and be able to demonstrate compliance with the principles outlined in this section 5.5.
   1. LSL Group’s policy on meeting the requirements of these principles is set out in the following sections [6](#_bookmark1) to [13.](#_bookmark6)

# Principle 1 – Lawfulness, fairness and transparency:

* 1. Personal Data must be processed fairly, lawfully and in a transparent manner.
  2. Generally speaking each LSL Group company should only process Personal Data where:
     1. it is necessary for the purpose of its legitimate business interests (and does not prejudice the privacy rights of the Data Subjects involved); or
     2. the individual concerned has consented to the particular use of their Personal Data.
  3. Each LSL Group company should only process Special Category Personal Data where:
     1. the Data Subject concerned has explicitly consented to the particular use of their data;
     2. the Processing is required to meet the LSL Group company's obligations under employment law; or
     3. the Processing is in the substantial public interest to be able to provide vital insurance products as permitted by the DPA.
  4. In addition each LSL Group company should only process Personal Data relating to criminal convictions and offences where:
     1. this is expressly authorised by law; and
     2. provided the LSL Group company comply with any additional safeguards set out in the law which authorises the processing.
  5. If the LSL Group company has any doubts as to whether the requirements of sections [6.2](#_bookmark2) , [6.3](#_bookmark3) and 6.4 are likely to be satisfied they are to contact their relevant DPS. There are additional conditions for Processing (and exemptions) which may be applicable and the DPS will be able to discuss these the LSL Group company.
  6. In addition LSL Group companies must:
     1. not use Personal Data in a manner that has a detrimental impact on the Data Subjects of that Personal Data unless the LSL Group company is able to fully justify the use (i.e. the LSL Group company would not be able to use the Personal Data where such use would cause detriment to the individual concerned without any legitimate justification);
     2. handle Personal Data only in ways Data Subjects of that data would reasonably expect; and
     3. not do anything unlawful with the Personal Data.
  7. LSL Group companies must be transparent about how they intend to use Personal Data and give individuals appropriate privacy notices when collecting their Personal Data.
  8. Any initiative that involves the collection and use of Personal Data should be discussed with the relevant DPS and may be referred to the Divisional DPO before launch to ensure that the necessary fair processing conditions will be met and that the appropriate privacy notices are provided to Data Subjects.

# Principle 2 – Purpose Limitation:

* 1. Personal Data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with that purpose or those purposes.
  2. In practice, the second data protection principle means that each LSL Group company must:

1. be clear and transparent from the outset about why it collects Personal Data and what the LSL Group company intends to do with it – each LSL Group company meets this requirement through the privacy notices it makes available to Data Subjects;
2. ensure that it maintains an accurate and up to date record which reflects the data Processing activities undertaken by that LSL Group company; and
3. ensure that if it wishes to use or disclose Personal Data for any purpose that is additional to or different from the originally specified purposes (as set out in the privacy notice provided to the relevant Data Subject(s)), the new use or disclosure is fair.
   1. If an LSL Group company wishes to use the Personal Data for a purpose which was not contemplated at the time of its collection, it will be necessary to consider whether this will be fair for the purposes of the GDPR. If using or disclosing the Personal Data would be unfair because it would be outside what the individual concerned would reasonably expect, or would have an unjustified adverse effect on them, then the use or disclosure is likely to be incompatible with the requirements of the GDPR.
   2. Each LSL Group company will need to get prior consent to use Personal Data for a purpose that is additional to, or different from, the purpose it was originally obtained for (or at the very least inform the individuals concerned of the new purpose). Any proposed new uses of the Personal Data held by a LSL Group company should be discussed with the relevant DPS to ensure that the new use meets the requirements of the GDPR.

# Principle 3 – Data minimisation:

* 1. Personal Data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
  2. In practice the third data protection principle means that each LSL Group company should:
     1. only hold Personal Data about the Data Subject that is sufficient for the purpose that LSL Group company is holding it for in relation to that Data Subject; and
     2. not hold more information than that LSL Group company needs for that purpose.
  3. Each LSL Group company must consider the minimum amount of Personal Data needed to fulfil the purpose for which it is being collected. Any data which is not necessary for that purpose should not be collected.

# Principle 4 – Accuracy:

* 1. Personal Data must be accurate and, where necessary, kept up to date.
  2. In practice the fourth data protection principle means that each LSL Group company must:
     1. take reasonable steps to ensure the accuracy of any Personal Data that it obtains;
     2. ensure that the source of any Personal Data is clear;
     3. carefully consider any challenges to the accuracy of any Personal Data; and
     4. consider whether it is necessary to update the Personal Data.
  3. It is also essential that each LSL Group company accurately collects and records customer consent data (where applicable). For example, residential sales and lettings branch staff must ensure that where consent is withheld or a customer opts out of marketing, it is correctly recorded on LSL Group systems and that the customer data is then not passed on for inclusion in any marketing campaigns or to any third parties.
  4. Please note that a customer can grant/withhold consent or opt-out of different methods of marketing communications. For example, a customer may be willing to accept marketing communications by email but refuse consent for telephone calls.

# Principle 5 – Storage Limitation:

* 1. Personal Data must not be kept for longer than is necessary for the purpose or purposes for which it is processed.
  2. In practice this means that Personal Data should be securely destroyed or erased from LSL Group systems when it is no longer required. For guidance on how long certain Personal Data is likely to be kept before being destroyed, please see the Data Retention Policy that is specific to the LSL Group company working environment or contact LSL Legal Services.
  3. Each of the Divisional DPOs are responsible for ensuring that a Data Retention Policy is documented for their companies/business areas.

# Principle 6 – Integrity and Confidentiality:

* 1. Principle 6 provides that appropriate technical and organisational security measures must be taken against unlawful or unauthorised Processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.
  2. The GDPR requires LSL Group companies to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.
  3. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the Personal Data, defined as follows:
     1. **Confidentiality** means that only people who are authorised to use the data can access it.
     2. **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is processed.
     3. **Availability** means that LSL Group companies should ensure timely and reliable access to and use of Personal Data. Personal Data should therefore be stored on our central computer system instead of individual PCs/laptops/iPads/iPhones/iPods and other devices unless such storage has been approved by the IT Team and appropriate encryption software is in place.
  4. Security procedures include:
     1. **Entry controls:** Any stranger seen in entry-controlled areas should be reported to your line manager and DPS, if appropriate this should be raised as a Data Security Incident.
     2. **Secure lockable desks and cupboards:** Appropriate regard should be given to keepingdesks and cupboards locked if they hold confidential information of any kind. (Personal Data is always considered confidential).
     3. **Methods of disposal:** The disposal of paper documents and memory devices (such as data sticks or CD-ROMs) should only be carried out by individuals nominated by the management team and in accordance with the LSL Data Disposal Policy.
        1. Paper documents should be disposed of securely for example by shredding or use of confidential disposal (e.g. blue bags/bins); and
        2. Memory devices (such as data sticks or CD-ROMs) should be physically destroyed when they are no longer required. Such items must be passed onto the relevant IT department for secure disposal.
     4. **Equipment:** Data Users should ensure that individual monitors do not show confidential information to passers-by and that they lock or log off from their PC laptop/iPad/iPhones and other devices when they are left unattended.
     5. **E-mail**: Where data users are using an email system which does not afford encryption protection, then great care should be taken in the transmission of any Personal Data, for example, by securing the data in a password protected file rather than in the body of the email. Where a member of staff is authorised by their LSL Group company to access emails on their own devices (e.g. laptop, phones or tablets), the member of staff is responsible for ensuring the following:
        1. Any device used to download email must be password/code protected and encrypted;
        2. Staff are responsible for the security of the LSL Group company emails and data on their device and must put in place appropriate security arrangements;
        3. Staff must not allow others to access the emails on the device;
        4. If the device is lost or stolen, the member of staff must notify the relevant Information Security Officer and/or the IT Team and arrange for the device to be remotely wiped; and
        5. Staff must ensure that the devices are backed-up using a secure and encrypted back up device.
     6. **Data Transfer:** Only memory sticks or other equipment supplied by the IT Team should be used to transfer any Personal Data. This equipment should be encrypted for storing Personal Data and under no circumstances should employees transfer any Personal Data on to their home/personal computers or other equipment. If Personal Data is being emailed, appropriate measures must be taken to ensure the transmission is secure.
     7. **Electronic Back-Up:** Anyone storing information locally on a laptop is responsible for the back- up of that data so that it can be restored in the event of a hardware failure. Back-ups should be taken on a regular basis to LSL Group supplied back-up devices only, which must be encrypted.
  5. Where Personal Data is being processed by a third party Data Processor on behalf of any LSL Group company, it is essential that either LSL Legal Services or the relevant Divisional DPO is consulted before any processing takes place and that a written GDPR compliant Data Processor agreement is put in place. In addition, appropriate due diligence checks must be completed before any Personal Data is disclosed to ensure that the LSL Group company has reviewed and satisfied itself with regard to the security arrangements that are in place. Once appointed, the Data Processors’ security measures must be regularly checked to ensure continued compliance with both the GDPR and the LSL Group requirements.
  6. Where Personal Data is being obtained from or shared with a third party Data Controller by any LSL Group company, the Divisional DPO should be notified and LSL Legal Services should be consulted to ensure that where appropriate a written data sharing agreement is put in place. In addition, appropriate due diligence checks should be completed before any Personal Data is obtained or disclosed to ensure that the arrangements have been reviewed and satisfied with regard to the security and data sharing arrangements that are in place. Once terms are agreed, regular due diligence checks should be undertaken to ensure continued compliance with both the GDPR and the LSL Group’s requirements.
  7. For further information and requirements concerning data sharing, see section [16.3](#_bookmark8) below.

Data Security Incidents

* 1. Where a LSL Group company fails to ensure that Personal Data is kept secure, this is known as a “**Data Security Incident**”. Some examples of a Data Security Incident are:
     1. loss of paper files containing Personal Data;
     2. sending an email containing Personal Data about an individual to a person or third party by mistake where that person or third party is not entitled or authorised to view that Personal Data; or
     3. failing to securely dispose of Personal Data contained in electronic form by not securely destroying the media on which the Personal Data is stored.
  2. Under the GDPR each LSL Group company is responsible for Data Security Incidents that involve third party Data Processors Processing Personal Data on behalf of any LSL Group company and these should be treated in the same manner as any other Data Security Incident and dealt with in accordance with the LSL Group Breach Notification Policy available on People Matters or relevant Divisional intranets.
  3. Further guidance on practical measures to ensure that Personal Data remains secure is available on People Matters or relevant Divisional intranets as well as guidance being made regularly available by the Divisional ISOs and DPOs. If any employee suspects or becomes aware of any Data Security Incident, they must ensure that their company/business unit’s DPS and the Divisional DPO as well as the Divisional ISO are notified without any delay and the procedure set out in the LSL Group Breach Notification Policy is followed. Notification will be made in accordance with the arrangements specified by the Divisional DPO or where applicable Divisional, incident management procedures. The Divisional DPO and the relevant DPS will ensure that the breach is dealt with in accordance with the GDPR, as well as determining whether it is necessary to notify the ICO of the Data Security Incident.

# Principle 7 - Accountability:

* 1. The accountability principle requires each member of the LSL Group to demonstrate that it can comply with the other 6 data protection principles outlined above. To demonstrate compliance each member of the LSL Group must:
     1. implement appropriate technical and organisational measures such as internal data protection policies, staff training and internal audits of processing activities;
     2. maintain relevant documentation on processing activities including a GDPR compliant written agreement when using a third party to process Personal Data on its behalf;
     3. appoint a data protection officer;
     4. implement measures that meet the principles of data protection by design and data protection by default, these could include:
     5. data minimisation;
     6. pseudonymisation: processing Personal Data in such a way that the Personal Data can no longer be attributed to a specific Data Subject without use of additional information and where such additional information is kept separately and is subject to appropriate technical and organisational measures to ensure that Personal Data are not attributed to an identified or identifiable living person;
     7. transparency;
     8. allowing individuals to monitor processing; and
     9. creating and improving security features on an ongoing basis.
     10. use data protection impact assessments where appropriate – further details on when use of a data protection impact assessment may be appropriate are set out in section 16 below.

# Rights of Data Subjects:

* 1. Personal Data must be processed in line with Data Subjects' rights. In the event that a Data Subject notifies an LSL Group company that it is exercising any of its rights (which are summarised below), the Divisional DPO must be immediately informed so that they can ensure that any Data Subject notification or request is dealt with in compliance with the GDPR. Individual employees must not respond to a Data Subject notification or request directly.
  2. In summary Data Subjects have a right to:
     1. **be informed** – you must provide ‘fair processing information’, typically through a privacy notice at the point you collect Personal Data from a Data Subject which explains how you intend to use the Personal Data in a concise, transparent, intelligible and easily accessible manner which is written in clear and plain language;
     2. **access –** please see section 14 below for details of the procedures to be followed in relation to this right;
     3. **rectification –** Data Subjects are entitled to have Personal Data rectified if it is inaccurate or incomplete;
     4. **erasure –** Data Subjects can request the deletion or removal of Personal Data where there is no compelling reason for its continued processing. It is not an absolute right and only applies:
     5. where the Personal Data is no longer necessary in relation to the purpose for which it was originally collected/processed;
     6. when the Data Subject withdraws consent and no other legitimate ground for processing applies;
     7. when the Data Subject objects to the processing and there is no overriding legitimate interest for continuing the processing;
     8. where the Personal Data was unlawfully processed (i.e. otherwise in breach of the GDPR); or
     9. where the Personal Data has to be erased in order to comply with a legal obligation.

There are also some specific circumstances where the right to erasure does not apply and a Data Subject can be refused a request;

* + 1. **restrict processing –** this right enables a Data Subject to ‘block’ or suppress processing of Personal Data. In these circumstances LSL Group companies are permitted to store the Personal Data but not further process it. LSL Group companies are required to restrict processing:
    2. where a Data Subject contests the accuracy of the Personal Data. The LSL Group company should restrict the processing until the accuracy of Personal Data has been verified;
    3. where a Data Subject has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and are considering whether legitimate grounds override those of the Data Subject;
    4. when processing is unlawful and the Data Subject opposes erasure and requests restriction instead; or
    5. if the LSL Group company no longer needs the Personal Data but the Data Subject requires the data to establish, exercise or defend a legal claim.
    6. **The right to data portability-** The right to data portability allows individuals to obtain and reuse their Personal Data for their own purposes across different services. It allows them to move, copy or transfer Personal Data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The right to data portability only applies:
    7. to Personal Data an individual has provided to a Data Controller;
    8. where the processing is based on the Data Subject’s consent or for the performance of a contract; and
    9. when processing is carried out by automated means.
    10. **The right to object –** Data Subjects have the right to object to processing based on legitimate interests, direct marketing (including profiling) and processing for purposes of scientific/historical research and statistics.Where an objection is made to processing based on legitimate interests the LSL Group company must stop processing the Personal Data unless it can demonstrate a compelling legitimate ground for the processing which overrides the interest of the Data Subject or the processing is for the establishment, exercise or defence of legal claims. There are no exemptions or grounds to refuse a Data Subjects objection to processing for direct marketing purposes.
    11. **Rights in relation to automated decision making and profiling –** Data Subjects have the right not to be subject to a decision based solely on automated processing (decisions which do not involve any human involvement), including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. LSL Group companies can only carry out solely automated decision-making with legal or significantly similar effect if the decision is:
    12. necessary for entering into or performance of a contract between the LSL Group company and the Data Subject;
    13. authorised by law; or
    14. based on the Data Subject’s explicit consent.
  1. LSL Group companies must give effect to each of the Data Subject rights set out at paragraphs 13.1.2 to 13.1.8 within one month of receipt of a valid Data Subject request to exercise such rights.

# Dealing with Subject Access Requests:

* 1. This section explains the procedures that LSL Group companies must follow when dealing with a Subject Access Request.
  2. A Data Subject (including an employee of any LSL Group company) has a right, on making a request to the Data Controller, to be informed whether Personal Data of which he is the Data Subject is being processed by or on behalf of that Data Controller (Article 15, GDPR).
  3. As well as having the right to receive a copy of the Personal Data undergoing processing, Data Subjects also have a right to the following information:

1. the purposes of the processing;
2. the categories of Personal Data concerned;
3. the recipients or categories of recipient to whom the Personal Data have been or will be disclosed;
4. where possible the envisaged period for which the Personal Data will be stored or if not possible, the criteria used to determine that period;
5. the existence of the right to request from the Data Controller rectification or erasure of Personal Data or restriction of processing or to object to processing;
6. the right to lodge a complaint with a supervisory authority;
7. where the Personal Data was not collected from the Data Subject, any available information as to their source;
8. the existence of automated decision-making including profiling and meaningful information about the logic involved as well as the significance and the envisaged consequences of such processing; and
9. where Personal Data are transferred to a third country or international organisation, the appropriate safeguards in place relating to the transfer.
   1. A Subject Access Request can take any form and could for example be submitted in writing by letter or an email or verbally face to face or over the phone. On receipt of a Subject Access Request, no fee may be charged for the provision of the information. Before agreeing to any request, identification details may be requested. Any member of staff who receives a written request should forward it to the Divisional DPO immediately. The GDPR stipulates a timetable for reply (one month from receipt of the request), so it is important that there are no delays in the DPO being advised of the request. A request that is received from a member of staff relating to their employment must be sent to Group HR ([mbhrsupport@lslps.co.uk](mailto:mbhrsupport@lslps.co.uk), or alternatively post to Group HR Operations Support Team, Newcastle House, Albany Court, Newcastle Business Park, Newcastle upon Tyne, NE4 7YB) or as provided in the Group HR Data Protection Policy.
   2. All staff must co-operate fully with the Divisional DPO to ensure that a compliant response is issued to any request.

# International data transfers:

* 1. Personal Data must not be transferred to a country or territory outside the European Economic Area (**EEA**) unless that country or territory ensures an adequate level of protection for Personal Data (the European Commission has made findings of adequacy with respect to a number of non-EEA countries) or an exemption applies. Broadly speaking, the EEA comprises the member states of the European Union, plus Iceland, Liechtenstein and Norway.
  2. Any transfer of Personal Data outside the EEA must be discussed with the Divisional DPO to ensure that the transfer is made in accordance with the GDPR. For these purposes, accessing Personal Data hosted in the EEA from a country outside the EEA will constitute a transfer.

# Data Protection Impact Assessments (DPIAs):

* 1. DPIAs help organisations to identify the most effective way to comply with their data protection obligations and meet individuals’ expectations of privacy allowing problems to be fixed at an early stage. The GDPR requires each member of the LSL Group to carry out a DPIA in the following circumstances:
     1. when using new technologies; and/or
     2. when the processing is likely to result in a high risk to the rights and freedoms of individuals.

* 1. Processing that is likely to result in a high risk includes (but is not limited to):
     1. systematic and extensive processing activities, including profiling and where decisions have legal effects – or similarly significant effects – on individuals.
     2. large scale processing of Special Category Data or Personal Data relation to criminal convictions or offences. This includes processing a considerable amount of Personal Data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity; and
     3. large scale, systematic monitoring of public areas (CCTV).
  2. In the event that a circumstance arises which may require a DPIA, the Divisional DPO must be immediately informed so that they can manage the process of completing a DPIA in accordance with the company’s DPIA procedure. Individual employees must not carry out a DPIA without the involvement of the DPO.

# Providing information over the telephone:

* 1. Any member of staff dealing with telephone enquiries must take great care when disclosing any Personal Data held by the LSL Group. In particular they should:
     1. Where this is possible, check the caller's identity by reference to the LSL Group company’s records to make sure that information is only given to a person who is entitled to it.
     2. Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
     3. Refer to the Divisional DPO for assistance in difficult situations. No-one should be bullied into disclosing Personal Data.

# Data Sharing Code of Practice (Code):

* 1. In May 2011, the ICO published a code of practice regarding Data Sharing (see definition below). The Code contains a number of good practice recommendations, which ensure that where the LSL Group company collect and share Personal Data, the LSL Group Company will do so in a manner that is fair, transparent and in line with the rights and expectations of the people whose information we are sharing.
  2. The Code is a statutory code (which means it has been approved by the Secretary of State and Parliament).

While it does not impose additional legal obligations, it can be used in evidence in any legal proceedings (not just the GDPR). The Code is the ICO’s interpretation of the requirements of the GDPR, containing advice on good practice and it is intended to provide practical guidance.

* 1. Data Sharing is defined as the disclosure of data from one or more organisations to a third party or the Sharing of data between different parts of the same organisation. Sharing Personal Data with a third party will generally fall into one of the following situations:
     1. Sharing Personal Data with a third party appointed to provide a service on behalf of an LSL Group company which involves handling Personal Data. For example, this would cover a company appointed by an LSL Group company to remove and securely shred our confidential waste paper or a company appointed to provide payroll services. The third party is likely to be a Data Processor and the GDPR requires the applicable LSL Group company to ensure that the third party provides sufficient security/protection for the Personal Data and there is a written contract in place with this third party containing, at a minimum, the provisions required by the GDPR before the LSL Group company provides them with any Personal Data. Paragraphs [11.5](#_bookmark4) and [11.6](#_bookmark5) above set out the approach that should be taken with such arrangements.
     2. Sharing Personal Data with a third party, such as the police or a business partner, where the third party uses the Personal Data for their own purposes (for example, investigating crime or marketing its goods and services). Personal Data may be shared on an ad hoc or on a routine basis. In either case, LSL Group companies must only share Personal Data with that third party where it is fair and lawful for us to do so, and in compliance with the GDPR (and all other applicable data protection legislation); where possible, a written contract should also be in place setting out the LSL Group company’s and the third party's respective roles and responsibilities in the data Sharing arrangement. Before sharing any Personal Data in this context, the LSL Group company must obtain the consent of the DPS.
  2. The principles concerning the transfer and Sharing of data apply to both the dealings with parties outside the LSL Group and to transfers between LSL Group companies. Any transfers of data between LSL Group companies must be in accordance with the GDPR and the Code.
  3. LSL and LSL Group companies are committed to considering and observing the Code to ensure that all instances of data Sharing are in compliance with the GDPR. Employees should refer all data sharing proposals to the applicable Divisional DPO to ensure that appropriate arrangements are put in place to ensure compliance.

# Direct Marketing and Cookies:

* 1. All LSL Group companies are required to comply with their company’s Privacy Policy, the GDPR, DPA and the PECR when carrying out direct marketing. The PECR supplements the GDPR and DPA and, among other things, governs unsolicited (i.e. not specifically requested by the Data Subject) electronic direct marketing communications made by electronic mail (including SMS), telephone and fax. In some instances, the provisions of the PECR mean that the consent of the individual is required before they are sent a direct marketing communication.
  2. There are different requirements for different types of marketing and the Divisional DPO and./or LSL Legal Services should be consulted before any new marketing initiative is launched to ensure that all of LSL marketing initiatives are compliant with the GDPR, DPA and the PECR.
  3. PECR also regulates the use of cookies (and similar technologies) by websites. Please see the LSL Cookies Policy for further information.

# Breach of the GDPR & this Policy:

* 1. If an LSL Group company fails to comply with the GDPR (and other legal requirements) in relation to the way in which an LSL Group company handles Personal Data, this may result in regulatory action being taken against that LSL Group company.
  2. The ICO enforces the GDPR and can issue an enforcement notice requiring an LSL Group company to take certain steps to comply with the GDPR. It is a criminal offence to fail to comply with an enforcement notice. Where there has been a serious breach of the GDPR, the ICO can impose a monetary penalty of up to 20,000,000 EUR, or up to 4% of its group’s total annual turnover in the preceding financial year, whichever is higher. If an LSL Group company breaches the GDPR, individuals who have suffered damage or damage and distress may also be entitled to compensation. In addition, the FCA also has powers to fine companies that it regulates.
  3. In certain circumstances, if an LSL Group company misuses Personal Data (for example, where an employee accesses and uses any Personal Data that an LSL Group company holds for any personal purposes) the employee may be committing a criminal offence under the GDPR.
  4. It is important that all LSL Group employees take responsibility for ensuring that they act in accordance with this policy and all related policies. Any breach of this policy by employees will be taken seriously and may result in disciplinary action. It may also result in an LSL Group company breaching the GDPR or other legal requirements. Serious breaches of this policy by employees may constitute gross misconduct which, following LSL’s disciplinary procedure, may result in termination of employment (where relevant).

# Related Policies:

This Policy forms part of the LSL Information Security Framework, copies of all relevant documents are available on People Matters, a relevant intranet site or from LSL Legal Services.

# Do’s & Dont's Summary:

* 1. **Do’s**
     1. Only use data for those purpose(s) that you have informed the individual about and where required obtain the relevant consent from the individual for such purpose(s).
     2. Collect and maintain Personal Data accurately and where relevant keep the information collected up to date.
     3. Ensure that documents which collect Personal Data include appropriate and relevant data protection wording and consents.
     4. Take care when recording any personal comments or opinions, they are Personal Data. You should keep information factual and avoid unsubstantiated opinions or comments.
     5. Ensure that information is only shared with individuals and organisations that are entitled to receive it.
     6. Follow Information Security guidance on security procedures, such as positioning terminal screens out of sight, keeping your password confidential and taking care with paper files and extracts of Personal Data.
     7. You must ensure that you comply with all of the policies included in LSL's Information Security Framework together with any additional information security arrangements notified from time to time.
     8. You must ensure that your desk is kept clear and that Personal Data is not left lying around and ensure all confidential wastepaper is disposed of correctly.
     9. Log/sign off your computer screen at all times when you are away from your desk or use an approved password-protected screensaver.
     10. Store memory sticks, computer disks or tapes containing Personal Data in a secure place (for example drawers or cabinets that can be locked) when not in use.
     11. Be careful when discussing matters that constitute Personal Data in any public place as conversations may easily be overheard (ideally such conversations should not take place in public).
     12. Before entering into any new arrangements or agreements which involve the Processing or Sharing of Personal Data, contact your DPO and/or LSL Legal Services to ensure that all relevant data protection considerations are taken into account and that where necessary privacy impact assessments are completed.

# Dont's

* + 1. Don’t contact customers for the purposes of direct marketing where the customer has not provided the appropriate consent to do so.
    2. Don’t disclose information unless you are able to verify the identity of the enquirer and are certain that he/she is entitled to receive the information that has been requested.
    3. Don't leave data lying around carelessly. This applies not only to paper and printouts but also to leaving computer screens logged/signed on when not in use or when you are away from your desk.
    4. Don't leave data on an unattended screen if an unauthorised person can see it.
    5. Don't use wastepaper containing Personal Data as scrap paper and take this away from the office for personal use.
    6. Don't tell anyone else your computer passwords. It is your personal responsibility to keep your computer passwords safe, they must be kept confidential.
    7. Do not store Personal Data on any portable device (including a laptop or USB device) unless the device is encrypted and the device should be stored securely when not in use.
    8. Don't record unprofessional comments on any computer or paper records. Remember that such comments may be the Personal Data of the individual who is the subject of your comments.

# Monitoring & Review of this policy:

This Policy will be reviewed annually and LSL will continue to review the effectiveness of this Policy to ensure it is achieving its stated objectives.

# This Policy was updated and approved on 9th August 2018

# Appendix

# Divisional DPO Contact Details

# Estate Agency

# Name: Helen Martin

# Email address: [Helen.Martin@lslps.co.uk](mailto:Helen.Martin@lslps.co.uk)

# Telephone Number: 07976 950191

# Surveying

# Name: Paul RayCollins

# Email address: Paul.Raycollins@esurv.co.uk

# Telephone Number: 07968 604655

# Financial Services (Advance Mortgage Funding Limited and First Complete Limited)

# Name: Jane Cross

# Email address: [Jane.Cross@primis.co.uk](mailto:Jane.Cross@primis.co.uk)

# Telephone Number: 07850 203626

# Financial Services (Personal Touch Financial Services Limited)

# Name: Raj Lyall

# Email address: [Raj.Lyall@primis.co.uk](mailto:Raj.Lyall@primis.co.uk)

# Telephone Number: 0121 767 1163