PRIVACY POLICY

Lynch Auctioneers, as data controllers, are committed to ensuring personal data is held privately and securely. We respect our clients right to privacy and comply with our obligations under the Data Protection Acts 1988 and 2003. This policy explains how we collect, use, process and disclose your information, including personal information and how we keep it secure.

At Lynch Auctioneers we acknowledge the eight rules of Data Protection:

1. **Obtain and process information fairly**

In our auctioneering business we request information for the following reasons:

Vendors:

- Contact details for informing of house progress
- Photo ID for proof of identification
- Utility bill for proof of house ownership
- May request bank account details for transfer of balance of booking deposit at end of sale

Purchasers:

- Initially contact details for informing of house progress
- If successful, proof of financial funds to purchase property

Landlords :

- Contact details for informing of house progress
- Photo ID for proof of identification
- Utility bill for proof of house ownership
- Bank account details for transfer of rent
- PPS No. for PRTB registration

Tenants:

- Contact details for keeping up to date on house progress
- Photo ID for proof of identification
- PPS No. for PRTB registration

Valuation clients:

- Contact details for keeping up to date on house progress
- Plans and maps of personal property

This information is held securely and with consent and is processed accordingly. We honour to gather the data fairly and fairly process the data also and we are committed to ensuring that a clients privacy is protected at all times.

2. Keep data only for one or more specified, explicit and lawful purposes

We only keep data for the above purposes which are specific, lawful and clearly stated and the data should only be processed in a manner compatible with that purpose.

. We ensure to inform clients the reason in which we are holding their data

. and that the purpose for which the data is being collected is a lawful one

3. Use and disclose data only in ways compatible with these purposes

Any use or disclosure must be necessary for the purpose for which we collect and keep the data.

We use the following test of compatibility:

. we endeavour to use the data provided to us only in ways consistent with the purpose for which they are kept.

. we do not disclose date to a third party without prior consent

Any processing of personal data is undertaken in compliance with the Data Protection Acts. This requires that, as a minimum, any such processing takes place subject to a contract between us and our clients. We, as the data controller, take reasonable steps to ensure compliance by the data processor with these requirements.

4. Keep it safe and secure

Appropriate security measures are taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.

The security of personal information is all-important, in that it is more significant in some situations than in others, depending on such matters as confidentiality and sensitivity and the harm that might result from an unauthorised disclosure. High standards of security are essential for all personal information. The nature of our security used takes into account what is available technologically, the cost of implementation and the sensitivity of the data in question.

Our security levels are as follows:

- access to central IT servers are restricted in a secure location to a limited number of staff;
- access to any personal data is restricted to authorised staff on a 'need-to-know' basis in accordance with a defined policy;
- access to computer systems are password protected with other factors of authentication as appropriate to the sensitivity of the information;
- back-up procedures are in operation for computer held data;
- all reasonable measures are taken to ensure that staff are made aware of our security measures, and comply with them;
- all waste papers, printouts, etc. are disposed of carefully, using an onsite shredder;
- the owner of our business is responsible for security and for periodic reviews of the measures and practices in place.
- All portable devices are password protected. All mobile phones have PIN login protection.
- All passwords must be secure and include both uppercase and lowercase letters, a number and a symbol. Passwords are changed regularly, as are PIN logins non mobile phones.
- All portable devices containing private, sensitive or confidential data must be encrypted. However, we do avoid where at all possible, to not have sensitive or confidential date on portable devices but sometimes this is unavoidable.
- Data on mobile devices is backed up regularly.
- All staff are informed to take great care when using portable devices in public areas.
- Anti-virus and firewall is kept up to date on all devices.
- Staff are informed to refrain from leavin portable devices in an unattended vehicle.
- Care of USB, CD's etc containing personal information must be stored in a secure location overnight. There is a locked cabinet in the office for storage and staff are informed to take extra care if using outside of the office and never leave unattended.
- Perimeter security – office is locked and only one door access.
- Computer location – Computers are positioned so screen may not be viewed by members of the public.
- Storage of files are in key locked filing cabinets in office.

5. Keep it accurate, complete and up-to-date

Apart from ensuring compliance with the Acts, we ensure that all date is accurate and complete and kept up to date by regular contact with clients where needs be.

We ensure that:

- our clerical and computer procedures are adequate with appropriate cross-checking to ensure high levels of data accuracy;
- personal data is kept up-to-date and is fully examined;
- there are periodic reviews and audits, to ensure that each data item is kept up-to-date.

6. Ensure that it is adequate, relevant and not excessive

We endeavour to obtain the minimum of amount of personal data that is required by us to complete a transaction. These required details are outlined in 1 above, depending on which service we are providing.

Periodic reviews are carried out of the relevance of the personal data sought from data subjects through the various channels by which information is collected, i.e. forms, website etc. In addition, we review any personal information already held and if needs to be held for any longer on our system.

7. Retain it for no longer than is necessary for the purpose or purposes

We hold personal data for as long as is necessary to complete transaction between us and our client. If there is no good reason for retaining personal information, then that information is routinely deleted.

Old information about former customers or clients, is checked and deleted accordingly of no longer required.

If we require keeping personal information to better our relationship with our client for longer than the transaction, we will obtain the customers consent in advance.

We ensure that files are regularly purged and that personal information is not retained any longer than necessary.

8. Give a copy of personal data to individuals, on request

On making an access request any individual about whom we keep personal data is entitled to:

- a copy of the data we are keeping about him or her;
- know the categories of their data and our purpose for processing it;
- know the identity of those to whom we disclose the data;
- know the source of the data, unless it is contrary to public interest;
- know the logic involved in automated decisions;
- data held in the form of opinions, except where such opinions were given in confidence and even in such cases where the person's fundamental rights suggest that they should access the data in question it should be given.

To make an access request the data subject must:

- apply to us in writing (which can include email);
- give any details which might be needed to help us identify him/her and locate all the information we may keep about him/her e.g. previous addresses.
- we do not charge for this service.

Right of Access.

We ensure that any clients inaccurate information is rectified or erased, personal data taken off a direct marketing or direct mailing list and client have the right to complain to the Data Protection Commissioner.

In response to an access request we apply the following:

- supply the information to our client with 40 days of receiving the request;
- provide the information in a form which will be clear our clients.

If we do not have information about the individual making the request we would tell them so within the 40 days.

We inform our clients at this point of their entitlement to complain to the Data Protection Commissioner about any refusal or delay in providing in the information.

Cookies

Our website uses "cookie" technology. "A cookie is a small file which is stored on a user's computer. They are designed to hold a modest amount of data specific to a particular client and website, and can be accessed either by the web server or the client computer. This allows the server to deliver a page tailored to a particular user, or the page itself can contain some script which is aware of the data in the cookie and so is able to carry information from one visit to the website (or related site) to the next"[1] Our cookies record the number of visitors to our site and tracks user sessions on the site. Cookies can be declined and can also be disabled.

[1] www.whatarecookies.com