Leeds Building Society

GDPR Privacy Standard – Applicants to Leeds Building Society vacancies

WHO WE ARE, HOW TO CONTACT US AND OUR DATA PROTECTION OFFICER
Leeds Building Society of 26 Sovereign Street, Leeds LS1 4BJ is a data controller of your Personal Data.

Our Data Protection Officer can be contacted by email at dpo@leedsbuildingsociety.co.uk or by writing to Data Protection Officer, Leeds Building Society, 26 Sovereign Street, Leeds LS1 4BJ. Reference in this document, to LBS, we, us and our means Leeds Building Society.

In this document, we refer to privacy notices by Fraud Prevention Agencies and Credit Reference Agencies. For further information, please see the relevant sections below.

We reserve the right to update this standard from time to time to keep it up to date. The most recent version of the standard is available from the HR department.

This standard describes how the Society will process your personal data when undertaking its recruitment and on-boarding processes. This can also include special category data, such as, for example, race, ethnic origin and religion.

INFORMATION WE COLLECT AND HOLD ABOUT YOU
To enable us to consider your application, we will collect certain information about you. Most of this will be provided by you when you make your application**.** This includes, but is not limited to:

- Your title, full name, contact details (including for instance your email address, home and mobile telephone numbers);
- Your home address and correspondence address (where this is different from your home address);
- Your date of birth;
- Your nationality;
- Your previous experience and employers and educational background;
- Information regarding your financial circumstances (such as whether you have had any defaults/County Court Judgements or have been insolvent);
- Information regarding whether you have, or have had, any criminal convictions; and
- Equality and diversity monitoring information (provided on a voluntary basis) for example information regarding your gender, race and religion.

We will also collect information through the selection/interview process, to validate your skills, competencies and behaviours for the role to enable us to make informed and objective recruitment decisions. This will include information via aptitude tests (where we require you to complete these), interview notes and psychometric assessments.

Where you are successful in your application to join the Society you will be required to complete our "on-boarding" process where we will collect further information about you. Most of this will be provided by you. This includes, but is not limited to:

- pre-employment checks through documents such as your passport, birth certificate, national insurance number, proof of address history;
- your bank account details;
- your qualification certificates, or certified copies;
- your choices in relation to your benefits package (for example, the level of pension contribution you wish to make, whether you wish to access certain colleague benefits as part of our Total Reward offering and whether you wish to join the Colleague Association);
- your emergency contact details;

- confirmation as to whether your employment with the Society is your primary employment, whether you receive any job related government benefits and whether you have any outstanding student loans;
- Uniform requirements (for colleagues working in our Branch Network);
- Disclosure and Barring Service (DBS)/Criminal Record checks (where relevant for your role); and
- Information relating to the Financial Conduct Authority's Fitness and Propriety requirements (where relevant for your role).

As part, of your application, we will also obtain **information from third party sources** (as applicable) such as, but not limited to:

- Personal information about your credit history which we obtain from Credit Reference Agencies (please see section below), including data which originates from:
    - Court Judgments Decrees; and
    - administration orders made publicly available through statutory public registers (for further information, see the section on 'Credit Reference Agencies' below);
- Information from Fraud Prevention Agencies (please see the section on 'Fraud Prevention Agencies below);
- Information from Recruitment Agencies (where you have instructed a recruitment agency to act on your behalf);
- Employment references from your previous/current employer; and
- Pre-employment checks, for example:
    - Information from Dow Jones regarding politically exposed people;
    - idenTT (passport validation); and
    - Information from the Disclosure and Barring Service following a DBS check (where relevant for your role).

CREDIT REFERENCE AGENCIES

In order to process your application, we will perform credit and identity checks on you with one or more credit reference agencies ("CRAs"). To do this, we will supply your personal information to CRAs and they will give us information about you. This will include information about your financial situation and financial history. CRAs will supply to us both public (including the electoral register) and shared credit, financial situation and financial history information and fraud prevention information.

We will use this information to:

- Assess your financial integrity as a potential colleague of the Society;
- Verify the accuracy of the data you have provided to us; and
- Prevent criminal activity, fraud and money laundering.

When we conduct a search via the CRAs, this will leave what is known as a 'soft footprint' on your credit file. Other organisations will not be able to see that we have made a search and this will have no impact on your ability to secure credit.

The identities of the CRAs, their role as fraud prevention agencies, the data they hold, the ways in which they use and share personal information, data retention periods and your data protection rights with the CRAs are explained in more detail in the separate leaflet titled 'Credit Reference Agencies Information Notice', which is included within the online applicant tracking system.

FRAUD PREVENTION AGENCIES

We will check your details against Cifas databases established for the purpose of allowing organisations to record and share data on their fraud cases, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct ("Relevant Conduct") carried out by colleagues.

The personal data you have provided, we have collected from you, or we have received from third parties will be used to prevent fraud and other relevant conduct.

Details of the personal information that will be processed include: name, address, date of birth, any maiden or previous name, contact details, document references, National Insurance Number, and nationality. Where relevant, other data including employment details will also be processed.

We and Cifas may also enable law enforcement agencies to access and use your personal data to detect, investigate, and prevent crime.

We process your personal data on the basis that we have a legitimate interest in preventing fraud and other Relevant Conduct in order to protect our business and customers and to comply with laws that apply to us. This processing of your personal data is also a requirement of your employment with us.

Cifas will hold your personal data for up to six years if you are considered to pose a fraud or Relevant Conduct risk.

CONSEQUENCES OF PROCESSING FOR FRAUD PREVENTION PURPOSES
Should our investigations identify fraud or any other Relevant Conduct by you when applying for a role with us, any employment may be refused or your any employment may be terminated or other disciplinary action taken (subject to your rights under your existing contract and under employment law generally).

A record of any fraudulent or other Relevant Conduct by you will be retained by Cifas and may result in others refusing to employ you. If you have any questions about this, please contact the HR team.

DATA TRANSFERS BY CIFAS
Should Cifas decide to transfer your personal data outside of the European Economic Area, they will impose contractual obligations on the recipients of that data to protect your personal data to the standard required in the European Economic Area. They may also require the recipient to sign up to a code of conduct intended to protect your personal data.

WHAT ARE THE LEGAL GROUNDS FOR PROCESSING YOUR PERSONAL INFORMATION (INCLUDING WHEN WE SHARE IT WITH OTHERS)?

Under data protection laws, we can only process your personal data for certain reasons (including where we share it with other organisations).

Below, we set out these reasons:

1. **Processing is necessary to perform our contract with you or for taking steps prior to entering into it (during the application stage) or to comply with our legal obligations:**
    a) In order to enter into a contract with you and to comply with our legal obligations, we will process your personal information, as set out:
        - during all stages relevant to assessing and managing your application during the recruitment process;
        - to administer our governance requirements such as internal reporting and compliance obligations;
        - to carry out identity checks, anti-money laundering checks, and checks with Fraud Prevention Agencies;
        - to process information about a crime or offence and proceedings related to that (in practice this will be relevant if we know or suspect fraud);
        - to deal with requests from you to exercise your rights under data protection laws; and
        - where we carry out profiling and/or automated decision making (see below for further information regarding profiling and automated decision making).
    b) We will share your personal information as set out below:
        - with other third party suppliers who provide a service on our behalf relating to the recruitment process for, example online selection aptitude test providers, our regulators, where we are required to disclose information relating to the job you

undertake, for example those colleagues within the Strengthening Accountability in Banking Regimes;
- with Credit Reference Agencies in order to carry out identity and credit checks;
- with law enforcement agencies and governmental and regulatory bodies such as Fraud Prevention Agencies, the Financial Conduct Authority (FCA), the Prudential Regulation Authority (PRA), and the Information Commissioner's Office;
- Courts and other organisations where it is necessary for the administration of justice, to protect vital interests and to protect the security or integrity of our business operations;
- to any employer from whom we seek a reference about you;
- to anyone to whom we transfer or may transfer our rights and duties under our contract of employment with you; and
- where we have a duty to do so, or if the law allows us to do so.

2. **Legitimate Interests:**
The UK's data protection laws allow the use of personal data where its purpose is legitimate and isn't outweighed by your interests, fundamental rights or freedoms as a data subjects.
   a) We will use your personal information for the following legitimate interests:
      - to carry out monitoring and to keep records;
      - for management and audit of our recruitment systems and processes in seeking to appoint talent to our workforce;
      - For analysis and developing statistics;
   b) We will share your personal information as set out below with:
      - other organisations and businesses who provide services to us such as back up and server hosting providers, IT software and maintenance providers, document storage providers and suppliers of other back office functions; and
      - all representatives as part of any restructuring or sale of our business or assets.

3. **Processing with your consent:**
   a) When you request that we share your personal information with someone else and you consent to that; and
   b) When we process special category data such as information about your health (see below for further information).

4. Processing for a **substantial public interest** under laws that apply to us where this helps us to meet our broader social obligations such as:
   a) Processing special category data such as information about your health (see below for further information); and
   b) Processing that we need to do to fulfil our legal obligations and regulatory requirements.

DO WE PURCHASE DATA ON COLLEAGUES FROM THIRD PARTIES?
We do not purchase data about applicants or colleagues from third parties.

DO WE SHARE PERSONAL DATA INFORMATION WITH THIRD PARTIES, FOR MARKETING PURPOSES?
We do not share information with any third party for the purpose of marketing to you, without your consent.

DO WE COLLECT SPECIAL CATEGORY DATA?
Special category data includes information such as an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

We will collect special category data for equality and diversity monitoring, where you have provided consent for us to do so.

The Society adopts a standard of equal opportunity and no person(s) applying for employment with the Society will be treated less favourably than any other person(s) because of gender, sexual orientation, marital or civil partner status, race, religion or belief, colour, nationality, disability or age, ethnic or national origin.

IS YOUR PERSONAL INFORMATION TRANSFERRED OUTSIDE THE UK OR THE EEA?

We are based in the UK but sometimes your personal information may be transferred outside the UK or the European Economic Area. If it is processed within Europe or other parts of the European Economic Area (EEA) then it is protected by European data protection laws. Some countries outside the EEA do have adequate protection for personal information under laws that apply to us. We will make sure that suitable safeguards are in place before we transfer your personal information to countries outside the EEA which do not have adequate protection under laws that apply to us. Safeguards include contractual obligations imposed on the recipients of your personal information. Those obligations require the recipient to protect your personal information to the standard required in the European Economic Area. Safeguards also include requiring the recipient to sign up to a code of conduct to protect the personal information being transferred.

HOW IS YOUR DATA STORED?

We collate all recruitment data, with the exception of the most senior appointments, through our online recruitment platform, e-Arcu. Information relating to senior appointments is held confidentially by the HR Resourcing team within folders on the IT system, prior to the successful candidate being appointed.

HOW LONG IS YOUR PERSONAL DATA RETAINED FOR?

We store all applicant details on the applicant tracking system, e-Arcu, for a period of 24 months following receipt of your application form, when it is confidentially destroyed.

Successful applicant details are transferred to the organisation's HR systems during the pre-employment, on-boarding process.

DO YOU HAVE TO PROVIDE YOUR PERSONAL INFORMATION TO US?

We are unable to manage your employment contract and ongoing employment relationship with you without having personal information about you. Your personal information is required:

- before you can enter into the relevant employment contract with us;
- during the life of that employment contract; and
- it is required by laws that apply to us.

PROFILING AND OTHER AUTOMATED DECISION MAKING

This section is relevant where we make decisions about you using only technology, and where none of our employees or any other individuals have been involved in the process.

We can do this activity based only where the profiling and other automated decision making does not have a legal or other significant effect on you.

We make a small number of automated decisions during the application process to determine your eligibility to work in a financially regulated environment, based on the following questions:

- Do you have the right to work in the UK?
- Do you have any unsettled CCJs?

There is a legal justification to enable us to enter into a contract of employment and/or to ensure that a colleague has sound financial integrity as determined by our regulator(s).

WHAT ARE YOUR RIGHTS UNDER DATA PROTECTION LAWS?

Here is a list of the rights that all individuals have under data protection laws. These include:

- The **right to be informed** about your processing of your personal information;
- The right to have your personal information **corrected if it is inaccurate** and to have **incomplete personal information completed**;
- The right **to object** to processing of your personal information;
- The right **to restrict processing** of your personal information;
- The right **to have your personal information erased** (the *"right to be forgotten"*);

- The right to **request access** to your personal information and to obtain information about how we process it (please see below for further information);
- The right to **move, copy or transfer your personal information** (*"data portability"*);
- Rights in relation to **automated decision making which has a legal effect or otherwise significantly affects you**.

For further information about your rights, you can down our leaflet "Your Data Protection Rights" from the HR Hub on COLLIN.

You also have the right to complain to the Information Commissioner's Office who regulates data protection laws: https://ico.org.uk/.

HOW TO GET A COPY OF YOUR PERSONAL INFORMATION (DATA SUBJECT ACCESS REQUEST)
You can obtain a copy of your personal information held by us by contacting the Human Resources department hradmin@leedsbuildingsociety.co.uk or by writing to us at Data Subject Access Request, HR Operations team, Human Resources department, Leeds Building Society, 26 Sovereign Street, Leeds, LS1 4BJ. We'll deal with your request as quickly as possible but in no more than 1 month from receipt of all required information.

DATA ANONYMISATION AND USE OF AGGREGATED INFORMATION
Your personal information may be converted into statistical or aggregated data which means it can no longer be used to identify you. It may then be used to produce statistical research and reports.

DEFINITIONS
We explain below some of the key terms used in this document

Automated decision making	means process where we make decisions about you, such as your suitability for a product, using a computer based and automated system without a person being involved in making that decision (at least first time around).
Personal information	means information that is about you or from which we can identify you.
Profiling	means any form of automated processing of your personal information to evaluate certain personal aspects about you, such as to analyse or predict aspects concerning your economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Process, p**rocessing or processed**	includes everything we do with your personal information from its collection, right through to its destruction or deletion when we no longer need it. This includes for instance collecting it (from you), obtaining it (from other organisations), using, sharing, storing, retaining, deleting, destroying, transferring it overseas.
Legitimate interests	data protection laws allow the Processing of Personal Data where the purpose is legitimate and is not outweighed by your interests, fundamental rights and freedoms.