Privacy Notice

1. Objective

This Notice is a statement whereby we at Cairde Credit Union commit to protecting the rights and privacy of individuals in accordance with the Data Protection Act, 2018 (the Act) requirements and the General Data Protection Regulation 2016/679 (GDPR).

We are a data controller. As a data controller, we respect and protect the privacy of all individuals whose data we process. We ensure that all processing of personal data is carried out in line with the principle of data processing and our obligations as a data controller.

Our long form Privacy Policy is available online at www.cairdecu.ie with further information on the details provided in this Notice. Alternatively you can contact us using the details at the end of this notice with any queries.

2. Data Protection Principles

The law outlines specific principles relating to the processing of personal data and states that we, as a Data Controller, must ensure that personal data shall be:

- collected and processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with the Act and GDPR, not be considered to be incompatible with the initial purposes (**'purpose limitation'**);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**);
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the Act and GDPR subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**);
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**'integrity and confidentiality'**)

The Data Controller (Cairde Credit Union) shall be responsible for, and be able to demonstrate compliance with, the above listed principles (‘**accountability**’).

3. Rights of the Data Subjects

You have a number of rights around the personal data we collect, process and store, including relating to you. Please note that the above rights are not absolute, and some restrictions and limitations may apply. These rights are to:

- Be kept informed. This includes details on how your data is collected, used and secured,
- Request a copy of your personal data by way of a subject access request,
- Rectify and update your personal data,
- Request the erasure of your personal data,
- Object to the processing of your personal data,
- Restrict the processing of your personal data,
- Port your data to another organisation,
- Not be subject to automated decision-making including profiling, without human intervention being available,
- Lodge a complaint with the Data Protection Commission (www.dataprotection.ie)

Automated Loan Decisioning: We may use automated decision making as part of our loan/credit decision process, and which involves assessing your application for a loan, taking account of your current circumstances and evaluating your ability to meet the required repayments on the loan. The automated decision process involves assessing the following:

Amount requested

- Repayment period
- Employment details
- Expenditure
- Income
- Dependents
- Existing loans
- Credit history

The Credit Union uses this information to apply internal credit assessment rules in a consistent manner, and ensures that your application for a loan is treated fairly and efficiently and what is believed to be consistent with your repayment capacity. This process is carried out solely by automated means without any staff involvement but only for loan applications within very specific thresholds.

Under data protection legislation, you have the right to obtain human intervention in relation to any decision made solely by automated means. In practice this means you have the right to have your loan application reviewed by a member of credit union staff in the event that a loan is refused using automated decision making. You will be informed if your loan decision was reached by automated means and you can contact us to challenge or review the decision.

4. Types of Personal Data Held

Depending on your interaction with us, we will collect different types of personal data which may include:

- General: name, address, date of birth, email, telephone numbers, photo;
- Financial data: bank account details, financial status and history, banking details and transactions, borrowings, debit card details and receipts;
- Contract data: details of the credit union products member hold with us, signatures, identification documents, salary, occupation, payslips, source of wealth, source of funds, Politically Exposed Status, accommodation status, mortgage details, previous addresses, spouse, partners, nominations, Tax Identification/PPS numbers, passport details, driver

license details, tax residency, beneficial owners information, medical information, tax clearance access number, parent/guardian information (for minor accounts)
- Data collected through interactions with credit union staff and officers: CCTV footage, telephone voice recordings, email correspondence, records of current or past complaints,
- Other data: photo or videos of prize winners, IP addresses, tracking information from cookies.
- Special Category Data: Health data relevant to the provision of insurance, biometric data if a member joins our credit union through our App.

In certain instances, an individual may supply us with information relating to another individual. This may occur in the following cases:
- Bank statements provided where the account is in joint names,
- Utility bills in joint names
- Personal information contained in sets of Business Accounts

In these instances, it is the responsibility of the individual providing the data to ensure the other named individual/s are aware their data is being shared and do not object to this.

5. Purposes for Processing Personal Data

Account Opening:

We will use personal data in order to carry out the following functions related to opening an account:
- To open and maintain an account;
- To give consideration to an application prior to approval;
- Verifying the information provided in the application;
- To comply with our legal obligations, for example anti-money laundering, to identify connected borrower, to identify a politically exposed person;
- To confirm tax residency for the purposes of the Common Reporting Standard;
- To meet our obligations under the Credit Union's Standard Rules;
- To provide members with details of the Deposit Guarantee Scheme;
- To enable members to apply for a Current Account and Debit Card;
- To contact members in respect of their accounts;
- To contact members in relation to any operational matters within the credit union;
- To record details of nominations and to process the nomination (subject to a valid nomination) and transfer any nominated property to the nominee(s);
- To issue members with information on any product or service held at the Credit Union or to provide details of other services, products, offers or competitions that may be of interest to our members.

Loans: Applications, Administration and Arrears:

We will use personal data in order to carry out the following functions:
- Assessing a loan application and determining creditworthiness for a loan;
- Verifying the information provided in the application;
- Conducting credit searches and making submissions to the Central Credit Register;
- To purchase loan protection from ECCU;
- To determine whether an applicant is a connected borrower or related party borrower in order to comply with Central Bank Regulations;

- Administering the loan, including where necessary, to take steps to recover the loan or enforce any security taken as part of the loan;
- To take steps to secure repayment of a loan such as processing a charge on a property;
- Providing updates on loan products and services by way of directly marketing to members;
- To contact members regarding a loan enquiry submitted through our website or online advertising;
- To contact members in relation to any transactions or missed payments on their account;
- Meeting legal and compliance obligations and requirements under the Rules of the Credit Union;
- To complete a submission to the Central Credit Register where a loan falls into arrears;
- To thank members for completing their loan payments in full;
- To enable members to avail of AIS (Account Information Service) process to share their bank account transactions with us as part of a loan application. This process is carried out by an Independent Data Controller (Truelayer) and consent will be obtained by Truelayer;
- Where there is a breach of the loan agreement we may use the service of a solicitor to recover the debt. We will pass them details of the loan application in order that they make contact and details of the indebtedness in order that they recover the outstanding sum;

Guarantors: As part of the conditions of a loan, the appointment of a guarantor may be a requirement in order to ensure the repayment of a loan. In such instances, we have a legal and regulatory requirement to collect, process and store certain personal data of the guarantor. This will include data such as:

- name, address, contact details, occupation, salary and other relevant financial data.

The purposes for which we may process the data of the guarantor include:

- ensure the terms of the loan agreement are met
- to contact the guarantor if the loan falls into arrears or there is a change in the payments by the member that indicate a change in circumstances
- to collect the debt
- to carry our required credit searches

Please note that from 1st February 2025 we are required by law to carry out credit checks on the CCR on loan guarantors as well as loan applicants.

The loan balance may be communicated to the guarantor at any time for the duration of the loan. The details of the guarantor will be retained in line with the loan which is 7 years from the date the loan is paid in full.

General Administration and Operation

We will use personal data to assist it in carrying out the following:

- To record telephone conversations to offer individuals additional security, resolve complaints and improve service standards;
- To contact members to thank them for their custom, particularly in relation to the completion of a loan;
- To contact members, using any contact method supplied, about reactivating dormant accounts;
- When we issue a debit card and for the administration of a current account held in our Credit Union;

- To record CCTV footage to ensure the safety and security of our staff, members, volunteers and any other third parties visiting our premises, to resolve complaints and improve service standards;
- To collect certain personal data if members attend the AGM such as name, account number and signature;
- To issue obligatory information to members (eg. AGM notifications, annual accounts and certain reports);
- To collect member preferences regarding marketing materials;
- Providing updates on our products and services by way of directly marketing to members;
- From time to time we may collect a small amount of personal data for entry into competitions and prize draws e.g. Car Draw. We will only use this data for the purpose of determining entry and selecting a winner for the competition/draw. Any photographic images or videos processed during participation in competitions or draws will only be done so with specific consent;

We may process data for purposes that are not specifically outlined above. If we do, we will clearly outline the purposes at the time of collecting data. We will endeavor to explain these purposes when we collect this data. We use personal information for the purpose it was collected. We do not use personal information for any different purpose other than for what it was obtained for without notification and seeking permission first.

Online Operations

We offer a number of online services to our members and prospective members. In order to avail of our online services, members or prospective members must provide certain personal information.

This information is required to:

- Login to the online platform;
- Use our Mobile App;
- Transfer funds;
- Manage payments and payees;
- Apply for a loan;
- Upload loan supporting documentation;
- Upload updated ID and POA documents;
- Sign a credit agreement,
- Apply for membership of the credit union; and
- Upload documentation required a membership stage.

Specific Terms and Conditions apply to the usage of our online platforms, and we would advise users to read these and contact us with any queries.

Operation of our Website

Through the operation of our website, we process certain personal information depending on how visitors use our website. This may include:

- Personal data submitted to us through any of our online services listed above,
- Completing forms on our website including: Volunteer Application Form, Non-Member Enquiry Form, Current Account Application Forms, Membership Forms.

Data collected through our website will only be used for the specific purpose it was provided.

"Special Categories" of Data

In order to provide certain services, it may be necessary for us to process some "special categories" (see definition above) of personal data. "Special categories" of particularly sensitive personal data require higher levels of protection.
We need to have further justification for collecting, storing and using this type of personal data. We may process special categories of personal data in the following circumstances:

- In limited circumstances, with explicit written consent;
- Where you opt to join our credit union via our Mobile App, you will be asked to consent to the use of biometric data to carryout automated facial verification;
- Where we need to carry out our legal obligations and in line with our data protection policy;
- Where it is needed in the public interest, and in line with our data protection policy;
- We may process this type of information where it is needed in relation to legal claims or where it is needed to protect a member's interests (or someone else's interests) and a member is not capable of giving their consent, or where this information has already been made public;
- In certain circumstances, where a member becomes unable to transact on their account due to a mental incapability and no person has been legally appointed to administer the account, the Board may allow payment to another person who it deems proper to receive it, where it is just and expedient to do so, in order that the money be applied in the member's best interests. To facilitate this, medical evidence of the member's incapacity will be required which will include data about their mental health. This information will be treated as strictly confidential.

6. Data Sharing and Data Transfers

We do not sell any personal information, nor do we share it with unaffiliated third parties unless we are required to do so by law. We will ensure that any information passed to third parties conducting operational functions on our behalf will be done with respect for the security of personal data and will be protected in line with data protection law.
Ways in which we may share personal information include:

- With official bodies including, but limited to:
  - the Irish League of Credit Unions (ILCU) under the ILCU Standard Rules and the League Rules which govern the operation of Credit Unions;
  - ECCU Assurance DAC who provide Loan Protection and personal data must be shared in order to administer claims or deal with insurance underwriting;
  - The Central Credit Register who provide financial institutions with credit details relating to a member's eligibility for a loan;
  - The Central Bank of Ireland enforce certain reporting, compliance and auditing on Credit Unions. We are obliged, further to Central Bank Regulations, to identify where borrowers are connected in order to establish whether borrowers pose a single risk. We are also obliged to establish whether a borrower is a related party when lending to them, i.e. whether they are on the Board/Management Team or a member of the Board/ Management teams family or a business in which a member of the Board /Management Team has a significant shareholding;
  - Government Departments such as Department of Finance and the Department of Social Protection may require the Credit Union to share certain personal information in order to meet legislative and regulatory requirements;

  - The Revenue Commissioners impose certain reporting obligations on Credit Unions under the Common Reporting Standards in relation to tax residency and the in respect of dividend or interest payments to members.
- To engage external IT providers so as to ensure the security of our IT systems in order to protect all personal data;
- With our insurers or assessors when providing or reviewing information in the event of an incident occurring;
- To engage professional services of third parties, such as auditors, solicitors or any other such business advisers. Any such parties are bound by confidentiality;
- to offer debit card services to our members, we have partnered with PAYAC who act as Appointed Coordinators and Programme Managers;
- We reserve the right to report to law enforcement any activities that we, in good faith, believe to be illegal;
- If we issue you with a debit card, Transact Payments Malta Limited (which is an authorised e-money institution) will also be a controller of your personal data. In order for you to understand what they do with your personal data, and how to exercise your rights in respect of their processing of your personal data, you should review their Privacy Policy which is available here http://currentaccount.ie/files/tpl-privacy-policy.pdf
- If you avail of the AIS process as part of a loan application, you will be sent a link to the provider's portal (Truelayer Ireland Limited) where you will be asked to consent to retrieve your bank account information and to share this with the Credit Union. For the purposes of this process, Truelayer are an independent data controller and you can find full details about this process our website.
- With any relevant, authorised third parties as part of a merger or acquisition, any such parties will be bound by a duty of confidentiality;
- To provide information to An Garda Síochána (eg. CCTV footage) or other Government bodies or agencies when required to do so by law; and
- To transfer data to another credit union where we have received a request, authorised by you, from another credit union to do so.
- To operate video embedding with Vimeo on our website. Visitors must consent to certain cookies in order to view these videos.

There may be circumstances where we transfer your personal data outside the EEA, such as when we use the services of online platforms or where we use a cloud-based IT system to hold your data. We safeguard your data by ensuring a minimum of one of the following safeguards is in place:

- a contract based on "model contractual clauses" (also called Standard Contractual Clauses) approved by the European Commission, obliging them to protect your personal data; or
- with companies located in a third country approved by the European Commission under an adequacy decision, such as the UK.

Where any of our suppliers engage the service of sub-processor to process data of which we are a Data Controller, our due diligence measures will include an assessment of this processor, in particular where the processor is located outside the EEA.
Existing third parties located in the US that are involved in the processing of personal data are:

- DocuSign – for digital signatures through the online banking facility
- Vimeo – for video embedding on the www.cairdecu.ie website

Appropriate security measures and contractual agreements are in place to protect your data whenever it is shared with any third parties.

7. Lawful Basis for Processing Personal Data

We are obligated to define a lawful basis for processing personal data. Below is a summary of our use of personal data and the lawful basis we rely on for the processing different categories of data for different purposes.

- Article 6.1(b) "*processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*"
  Examples of where this lawful basis is applicable include the following:
  - the processing is necessary for us to setup and manage accounts and provide all services provided to our members;
  - for the purpose of assessing any loan application, processing applications individuals make and to maintain and administer any accounts held with the credit union;
  - to take steps to secure repayment of a loan where a loan goes into arrears;
  - to apply for Loan Protection;
  - to process a credit assessment when a member applies for a loan;
  - to apply for and obtain a debit card and to administer a current account;
  - to perform any part of a contract as per the Terms and Conditions outlined to our members in any such process.

- Article 6.1(c) "*processing is necessary for compliance with a legal obligation to which the controller is subject*"
  Examples of where this lawful basis is applicable include the following:
  - to comply with the all regulations as outlined in the Credit Union Act 1997 (as amended);
  - to meet our duties to the Regulator, the Central Bank of Ireland;
  - to fulfil reporting obligations to Revenue related to a member's tax liability under Common Reporting Standard;
  - to comply with anti-money laundering and combating terrorist financing obligations under The Money Laundering provisions of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2018, as amended by Part 2 of the Criminal Justice Act 2013;
  - to meet our legislative and regulatory duties to maintain audited financial accounts;
  - to comply with credit reporting obligations;
  - to comply with Connected/Related Party Borrowers obligations;
  - to appoint a person to administer an account where a member becomes mentally incapacitated;

- Article 6.1(f) "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party*"
  Examples of where this lawful basis is applicable include the following:
  - assessing a loan application, as well as fulfilling a contract mentioned above, the credit union also utilises credit data from credit referencing agencies. Our legitimate interest: The credit union, for its own benefit and therefore the benefit of its members, must lend responsibly and will use credit scoring information in order to determine suitability for a loan. We will also review our member's credit history on our database to assess each members past history and suitability for future lending. We will do so to ensure we lend responsibly and protect the financial stability of the credit union;

- when carrying out searches relating to credit worthiness. Our legitimate interest: The credit union, for its own benefit and therefore the benefit of its members, must lend responsibly and will use credit scoring information in order to determine loan suitability;
- CCTV recording on our premises. Our legitimate interest: it is necessary to secure the premises, property herein and any staff /volunteers/members or visitors to the credit union and to prevent and detect fraud;
- voice recording through phone conversation both incoming and outgoing. Our Legitimate interest: To ensure a good quality of service, to assist in training, to ensure that correct instructions were given or taken due to the nature of our business and to quickly and accurately resolves any disputes;
- during a recruitment process when we need to communicate with candidates. Our Legitimate interest: to update candidates on the recruitment process for the purposes of considering them for employment or for future positions;
- carrying out debt collection activities in the event of non-payment of a loan or missed payments. Our legitimate interest: we have a duty to our members to ensure the financial stability of the credit union so we must collect all amounts owed to us;
- carrying out data analytics. Our Legitimate interest: to ensure we are offering relevant services, to assess demand for certain services and to ensure we are acting in the best interests of the credit union to guarantee financial stability into the future. Data of individual accounts will not be analysed where individuals can be identified.

- Article 6.1(a) "*the data subject has given consent to the processing of his or her personal data for one or more specific purposes"*
  Examples of where this lawful basis is applicable include the following:
  - **Marketing**: to provide our members with details on our products and services provided they have not opted out of receiving such communications. Individuals can opt-out of receiving marketing communications at any time;
  - **Identification:** we request a member's consent to take a photo to store electronically on our database for the purpose of identification for their protection;
  - **Cookies on our website**: we may obtain information about general Internet usage by using a cookie file which is stored on an individual's browser or the hard drive of their computer. Visitors to our website can choose not to consent to cookies, or they can manage their cookie preferences, or they can select to opt-in to some or all types of cookies. We use a cookie management platform for this purpose. There are videos embedded on our website that will only operate when visitors consent to certain cookies. If consent is not given, the videos will not be visible. When a website visitor plays a video on our website, information such as IP address, Browser type (e.g. Mozilla Firefox, Google Chrome), Operating system (e.g. macOS, Windows), Clicking behaviour (the viewing of the video), Dwell time (How long does the visitor stay on the website) will be visible through the credit Union's account with Vimeo. We will only use this data in aggregate form for statistical purposes and never identify individual visitors.
  - **Competitions and Draws:** when members participate in competitions or draws they will be asked for their consent prior to their personal information or image being displayed on our website, social media platforms or other publications;
  - **Schools Quiz:** we participate in the Schools Quiz in liaison with the ILCU. The Schools Quiz is open to entrants aged 4 to 13. We will pass on a form to the contact in the

school who is then responsible for asking the entrants' parent/legal guardians for their consent to the processing of their child's personal data. This information is processed only where consent has been given;

- **AIS Process:** if a member avails of the AIS process as part of a loan application, the AISP (Account Information Service Provider) Truelayer Ireland Limited, will look for consent to consent to retrieve your bank account information and to share this with us. For the purposes of this process, Truelayer are an independent data controller.

- Article 6.1(e) *"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;"*
  Examples of where this lawful basis is applicable include the following:
  - Following guidelines from Public Health Authorities and Government in the event of any future pandemics.

8. Data Subject Access Requests (DSARs)

An individual has the right to be informed whether we hold data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request to us in writing and we will accede to the request within one month having first verified the identity of the requester to ensure the request is legitimate. Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the controller whether or not it needs to comply with the second request. This will be determined on a case-by-case basis. In cases where we process a large quantity of information concerning the data subject, we may request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable we must refuse to furnish the data to the applicant.

A Subject Access Request Form is available on our website www.cairdecu.ie. Individuals are asked to complete this form when making a DSAR, though it is not mandatory. Once we have verified the identity of the requester and the request is not deemed to be manifestly unfounded or excessive, we will comply with the request at no charge to the data subject and within one month.

We have an internal procedure in place to handle all DSARs.

9. Security of Personal Data

We ensure the confidentiality, integrity, availability, and resilience of personal data when in use, transit and storage. We are obliged to protect the data from inadvertent destruction, amendment, loss, disclosure, corruption or unlawful processing and we have appropriate technical and organisational measures in place to ensure all data is secure.
We carry out regular testing of the resilience of our systems, regular staff training and ensure the highest level of IT security measures are in place to protect your data.

10. Data Retention

We will only retain your personal data for as long as necessary to fulfil the purpose(s) for which it was obtained, taking into account any legal/contractual obligation to keep it. Where possible we

record how long we will keep your data, where that is not possible, we will explain the criteria for the retention period. Once the retention period has expired, the respective data will be permanently deleted. As a general rule, your personal information will be retained for 7 years from the date your credit union account closed. Where you apply for a loan, the documentation required for this will be retained for a minimum of 5 years from the date the loan is completed. However, they may be circumstances where we must retain data for longer than these specified periods, but we will always have a defined legitimate basis for any extended retention.
We maintain a full Retention Schedule in our Records Management Policy.

11. Privacy by Design and Default

The regulation requires that all our systems and processes are compliant in nature. The use of Data Protection Impact Assessments (DPIA) will be conducted on any new project that involves the collection of personal data or special categories of personal data as well as any changes to existing projects where there are risks to the data.
The DPO is notified in the advance planning stages of any proposed new processes or technologies or changes to existing processes. This includes internal projects, product development, software development, IT systems, and any other type of processing where personal data is affected. This will ensure that any required DPIAs can be carried out and the findings reported to the Board where necessary prior to any action being taken.

12. Notification of Data Breaches

Article 4(12) GDPR defines a 'personal data breach' as:
"*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*"
Our staff are trained to recognise a breach and are instructed to inform their line manager immediately if they suspect a breach has occurred or have evidence of a potential breach. The line manager will then escalate it to senior management and the DPO as required.
We have a Personal Data Breach Procedure in place which will be followed by the DPO and relevant staff members in the event of a breach being reported either internally or from a third-party processor.

13. Data Protection Officer (DPO)

The role of the Data Protection Officer has been outsourced to O'Dwyer Power under a contract outlining the tasks of the DPO in assisting Cairde Credit Union in complying with data protection legislation. The tasks of the DPO are in keeping with those defined in Article 39 of the GDPR.
The Board of Directors of Cairde Credit Union are ultimately responsible for able to demonstrate compliance with the law. Management are responsible for ensuring that all personnel are trained in their obligations.

14. Contact Details

If you have any questions, concerns or suggestions related to the processing of your personal data, you can contact us using our details below:
Data Protection Officer, Cairde Credit Union, 3 – 6 Parnell Street, Dungarvan, Co. Waterford.
Email: dpo@cairdecu.ie Tel: 058 44088

You have a right to complain to the Data Protection Commissioner (DPC) in respect of any processing. This can be done through the DPC website: https://www.dataprotection.ie.