



# Data protection policy

## Context and overview

### Key details

- Policy prepared by: A. Walker (Director)
- Approved by board / management on: 22/02/2022
- Policy became operational on: 22/02/2022
- Next review date: 22/02/2024

### Introduction

Unity Credit Union Limited needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

### Why this policy exists

This data protection policy ensures Unity Credit Union Limited:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

### Data protection law

The Data Protection Act 1998 describes how organisations — including Unity Credit Union Limited — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date

5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

## People, risks and responsibilities

### Policy scope

This policy applies to:

- The head office of Unity Credit Union Limited
- All branches of Unity Credit Union Limited
- All staff and volunteers of Unity Credit Union Limited
- All contractors, suppliers and other people working on behalf of Unity Credit Union Limited
  
- It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:
  - Names of individuals
  - Postal addresses
  - Email addresses
  - Telephone numbers
  - ...plus any other information relating to individuals

### Data protection risks

This policy helps to protect Unity Credit Union Limited from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

### Responsibilities

Everyone who works for or with Unity Credit Union Limited has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

- The **board of directors** is ultimately responsible for ensuring Unity Credit Union Limited meets its legal obligations.

## Data accuracy

The law requires Unity Credit Union Limited to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Unity Credit Union Limited should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- Unity Credit Union Limited will make it **easy for data subjects to update the information** Unity Credit Union Limited holds about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

## Subject access requests

All individuals who are the subject of personal data held by Unity Credit Union Limited are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at [info@unitycreditunion.co.uk](mailto:info@unitycreditunion.co.uk). The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £0.00 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.