
# Data Protection Policy

## Introduction

LCC (LCC Communications Ltd) 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 LCC:

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

## Data Protection Law

The Data Protection Act 1998, and subsequent General Data Protection Regulation (GDPR) ((EU) 2016/679) introduced in May 2018 describes how organisations – including LCC – 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 GDPR is underpinned by five important principles. These say that personal data must:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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 not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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."

## PEOPLE, RISKS AND RESPONSIBILITIES

### Policy Scope

This policy applies to:

- The head office of LCC
- All staff and volunteers of LCC
- All contractors, suppliers and other people working on behalf of LCC.

It applies to all data that the Company holds relating to identifiable individuals.

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

### Data Protection Risks

This policy helps to protect LCC 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 LCC 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.

However, these people have key areas of responsibility:

- The Managing Director is ultimately responsible for ensuring that LCC meets its legal obligations and is responsible for:
    - Keeping up to date about data protection responsibilities, risks and issues

- Reviewing all data protection procedures and related policies on a regular basis
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Dealing with requests from individuals to see the data LCC hols about them (also called “subject access requests”).
- Checking and approving any contractors or agreements with third parties that may handle the Company’s sensitive data
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the Company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters
- Addressing any data protection queries from journalists or media outlets like newspapers
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

## GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those who need it for their work
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- LCC will provide training to all employees to help them understand their responsibilities when handling data
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the Company or externally
- Data should be regularly reviewed and updated, if it is found to be out of date, if no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the Managing Director if they are unsure about any aspect of data protection

## DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Managing Director.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer
- Data printouts should be shredded and disposed of securely when no longer required

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated servers, and should only be uploaded to an approved cloud computing service
- Servers containing personal data should be sited in a secure location, away from general office spare
- Data should be backed up frequently and backups removed from the premises.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and firewall.

## DATA USE

Personal data is of no value to LCC unless the business can make use of it. However, it is when personal data is accessed and use that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Personal data should never be transferred outside of the European Economic Area.

- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

## DATA ACCURACY

The law requires LCC 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 LCC 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.
- 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 LCC 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 request this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Managing Director at support@lcccommunications.com. The Managing Director can supply a standard required form, although individuals do not have to use this.

Individuals will not be charged for subject access requests unless these are deemed as repetitive. The Managing Director will aim to provide the relevant data within 30 days.

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

## DISCLOSING DATA FOR OTHER REASONS

In certain circumstance, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, LCC will disclose requested data. However, the Managing Director will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

## PROVIDING INFORMATION

LCC aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

This is available on request. A version of this statement is also available on the company's website.

## ACCESSING LCC's SHARED WIFI

LCC provide a shared WIFI service to a number of businesses in the area. LCC take the security and protection of both data and the network very seriously and therefore ensure the network completely separates each location with the use of different IP ranges. This ensures the IT equipment at one location is not visible to that at another location. Each location is also protected by a firewall.