

## **Data protection policy**

Context and overview

### **Key details**

- Policy prepared by:
- Approved by board / management on:
- Policy became operational on:
- Next review date:

Garry Wight

23/05/2018

24/05/2018

23/01/2019

### **Introduction**

Language in Action needs to gather and use certain information about individuals.

These can include students, suppliers, agency partners, 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 organisation's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures Language in Action :

- Complies with data protection law and follow good practice
- Protects the rights of staff, students and agency 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 — Language in Action Ltd — 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

### **Language in Action**

3

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 main office of Language in Action
- All seasonal centres of Language in Action
- All staff and volunteers of Language in Action
- All contractors, suppliers and other people working on behalf of Language in Action

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 which is needed for Safeguarding or Welfare purposes.

### **Data protection risks**

This policy helps to protect Language in Action 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 or volunteers for or with Language in Action has some responsibility for ensuring data is collected, stored and handled appropriately.

4

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 company Director and management team are ultimately responsible for ensuring that Language in Action meets its legal obligations.
- The Data Protection Officer, Garry Wight, is responsible for:
  - o Keeping the leadership team updated about data protection responsibilities, risks and issues.
  - o Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - o Arranging data protection training and advice for the people covered

by this policy.

- o Handling data protection questions from staff and anyone else covered by this policy.
- o Dealing with requests from individuals to see the data Language in Action holds about them (also called 'subject access requests').
- o Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
  - The IT Administrator, Garry Wight, is responsible for:
    - o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - o Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - o Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
  - The Company Director Madan Haree , is responsible for:
    - o Approving any data protection statements attached to communications such as emails and letters.
    - o Addressing any data protection queries from journalists or media outlets like newspapers.
    - o Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.