Microbee Environmental Ltd

Data Protection Policy

Scope

This policy applies to all working for or with Microbee Environmental and it to ensure that data is collected, stored and handled appropriately and in line with the data protection principles.

Objectives

- To comply with data protection law and follow good practice;
- To protect the rights of staff, customers and partners;
- To be open about how to store and process individuals' data;
- To protects itself from the risks of a data breach.

The Data Protection Act 2018 describes how organisations – including Microbee – 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 2018 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. be 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

This policy applies to all staff members and all contractors, suppliers and other people working on behalf of the company. 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
- and any other information relating to individuals.

This policy helps to protect Microbee from data security risks, including:

- Breaches of confidentiality (e.g. information being given out inappropriately)
- Failing to offer choice (e.g. all individuals should be free to choose how the company uses data relating to them)

- Reputational damage (e.g. the company could suffer if hackers successfully gained access to sensitive data)

The directors are ultimately responsible for ensuring that Microbee meets its legal obligations, and they must:

- Be aware of data protection responsibilities, risks and issues;
- Review all data protection procedures and related policies, in line with an agreed schedule;
- Handle data protection questions from staff and anyone else covered by this policy;
- Deal with requests from individuals to see the data that Microbee holds about them (also known as 'subject access requests');
- Check and approve any contracts or agreements with third parties that may handle the company's sensitive data.

For IT systems they must:

- Ensure all systems, services and equipment used for storing data meet acceptable security standards;
- Perform regular checks and scans to ensure security hardware and software is functioning properly;
- Evaluate any third-party services that the company is considering using to store or process data, e.g. cloud computing services.

Paper format data storage

Data on paper should be kept in secure place and be shredded and disposed of securely when no longer required.

Electronic data storage

Electronic data should:

- Be protected by strong passwords that are changed regularly and never shared between employees.
- Be stored on designated drives and servers, and should only be uploaded to approved cloud computing services (e.g. OneDrive, Simpro). These shall be sited in a secure location, away from general office space.
- Be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- 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 a firewall.

Subject Access Requests

All individuals who are the subject of personal data held by Microbee 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.

Disclosing Data for Other Reasons
In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Microbee will disclose the requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the directors and from the company's legal advisers where necessary.

Signed	
Name	Sofia Calderon Draper
Position	Director
Date	20 Jan 2025